Caveats for 12.4(20)T1 through 12.4(22)T4

- Resolved Caveats—Cisco IOS Release 12.4(22)T4, page 243
- Resolved Caveats—Cisco IOS Release 12.4(22)T3, page 263
- Resolved Caveats—Cisco IOS Release 12.4(22)T2, page 280
- Resolved Caveats—Cisco IOS Release 12.4(22)T1, page 308
- Resolved Caveats—Cisco IOS Release 12.4(22)T, page 357
- Resolved Caveats—Cisco IOS Release 12.4(20)T6, page 416
- Resolved Caveats—Cisco IOS Release 12.4(20)T5, page 423
- Resolved Caveats—Cisco IOS Release 12.4(20)T4, page 435
- Resolved Caveats—Cisco IOS Release 12.4(20)T3, page 462
- Resolved Caveats—Cisco IOS Release 12.4(20)T2, page 486
- Resolved Caveats—Cisco IOS Release 12.4(20)T1, page 538

Resolved Caveats—Cisco IOS Release 12.4(22)T4

Cisco IOS Release 12.4(22)T4 is a rebuild release for Cisco IOS Release 12.4(22)T. The caveats in this section are resolved in Cisco IOS Release 12.4(22)T4 but may be open in previous Cisco IOS releases.

- 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.

- CSCsm87925

  Symptoms: Memory leak occurs in SSGCmdQue.

  Conditions: Occurs on routers configured for Service Selection Gateway (SSG) and running Cisco IOS Release 12.4(15)T2.

  Workaround: There is no workaround.

- CSCso69413

  Symptoms: A Cisco router may reload when Flexible Packet Matching is configured.

  Conditions: This symptom occurs when a class is configured to match on a protocol field when the protocol stack has not been defined. The stack class- map is required for all field references.

  Workaround: Specify the exact bits to be matched with the **match start** command.

- CSCso97304

  Symptoms: Configuring and unconfiguring hierarchical QoS may cause memory leak on a Cisco router.

  Conditions: This symptom occurs on a Cisco router that is running Cisco IOS Release 12.4(15)T4.

Workaround: There is no workaround.

- CSCsq99299

  Symptoms: Router crashes during traceback generation with a bus error.

  Conditions: When CPUHOG occurs, traceback is generated. In some cases, it may lead to crash due to uninitialized internal data.

  Workaround: There is no workaround.

- CSCsr05431

  Symptoms: There is a traffic drop after an SSO.

  Conditions: The symptom is observed with high scaling, lots of VRFs, and a core with no load sharing. It is seen with two VRFs that are overloaded and slow due to the shared link.

  Workaround: There is no workaround.

  Further Problem Description: Use the graceful restart timer to increase the time that it takes the initial and subsequent peers to come up, before doing bestpath calculations.

- CSCsr60092

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

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

  Workaround: There is no workaround.

- CSCsu05306

  Symptoms: A Cisco device might report a crash because of a software-forced crash and/or bus error. The root cause for the crash: Refcount becomes –1 as the chunk was already freed.

  Conditions: This symptom is observed on a Cisco device only when an application firewall for HTTP inspection is turned on.

  Workaround: There is no workaround.

- CSCsu45780

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

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

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

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

- CSCsu50869

  Symptoms: Calls do not complete because Cisco Unified Border Element (CUBE) does not sent PRACKs to all 1xx messages.

  Conditions: Occurs 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 acknowledgments.

- CSCsu78975

  Symptoms: Crash seen @adj_switch_ipv4_generic_les on a Cisco 38xx router.

Conditions: This symptom is observed upon issuing the **no ip route 10.2.82.0 255.255.255.0 vlan1** command.

Workaround: There is no workaround.

- CSCsu92724

  Symptoms: The following errors are logged:

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

  Conditions: Occurs when ISDN is enabled.

  Workaround: There is no workaround.

- 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 issued.

  Workaround: There is no workaround.

- CSCsv62323

  Symptoms: The Fast Ethernet driver code may cause several errors. The observed symptoms of this issue include:

  - Cisco Unified Communications 500 series routers (UC520) may crash with an “Unexpected exception to CPU” error.
  - Cisco 1861 router may fail to establish L2TPv3 session with an error message:

```
“L2TP-3-ILLEGAL: _____:________: ERROR: unsupported transport protocol; defaulting
to UDP if possible”
```

  Conditions: The symptoms are observed with the following hardware platforms: UC520, Cisco 880 series, Cisco VG202, Cisco VG204, IAD2435-8FXS, and Cisco 1861 routers. In addition, the following conditions exist:

  - The UC520 must be configured with a BVI interface. For example:

```
interface BVI1
 ip address 192.168.0.1 255.255.255.0
```

  - The Cisco 1861 router is configured with L2TPv3. For example:

```
pseudowire-class l2tpv3
 encapsulation l2tpv3
 ip local interface Loopback0
!
interface Loopback0
 ip address 192.168.10.1 255.255.255.255
```

```
!
interface FastEthernet0
 no ip address
 xconnect 192.168.0.1 1 pw-class l2tpv3
```

Workaround: There is no workaround.

Further Problem Description: The issue is caused by an underlying driver vulnerability that exists in the UC520, Cisco 880 series, Cisco VG202, Cisco VG204, IAD2435-8FXS and Cisco 1861 routers. No other model of Cisco routers/switches are known to be affected by this issue. The symptoms can be triggered with specific TCP sequences.

- CSCsv91628

  Symptoms: BGP prefixes are not exchanged between route reflectors.

  Conditions: Occurs when route reflectors are present in different AS and they have MP-EBGP relationship between them.

  Workaround: There is no workaround.

- CSCsw39413

  Symptoms: The following sequence of steps used to reset all the C5510 DSPs on a Cisco C1861 voice gateway will leave DSP 1 in an unusable state, and all analog voice ports tied to this DSP for signaling channels will be forced into a shutdown state.

  (A) Invoke “test voiceport driver” for slot 0.
  (B) Choose the “2 - 5510 DSP test” option.
  (C) Select “1 - Reset ALL DSPs”.

  Conditions: This behavior is observed on Cisco C1861 voice gateways installed with any Cisco IOS release that supports these products, namely 12.4T and 12.4T-based Cisco IOS releases that support voice features.

  Workaround: The following alternate methods to reset all the C5510 DSPs have been observed to correctly bounce and recover both of the DSPs and all analog voice ports tied to DSP 1.

  Alternative 1:

  (A) Invoke “test voiceport driver” for slot 0.
  (B) Choose the “2 - 5510 DSP test” option.
  (C) Select “2 - Reset 1 DSP” twice, and each time specify DSP ID 1 or 2.

  Alternative 2:

  (A) Invoke “test voiceport driver” for slot 0.
  (B) Choose the “2 - 5510 DSP test” option.
  (C) Select “14 - faked dsp crash” twice, and each time specify DSP ID 1 or 2.

  Alternative 3:

  (A) At the EXEC prompt, issue the “test dsp device all all reset” command.

- CSCsw73196

  Symptoms: BGP MDT session flaps when a router running Cisco IOS is interoperating with a router running Cisco IOS-XR and when withdrawal messages are sent by IOS to XR of previously advertised MDT prefixes.

  Conditions: MDT prefixes need to be exchanged by IOS and XR routers. If a withdrawal message is exchanged subsequently for any reason then this problem is seen.

  Workaround: There is no workaround.

- CSCsw79891

  Symptoms: Cisco 3845 gateway may not detect an H.263 video during a video call.

  Conditions: The symptom is observed with a Cisco 3845 gateway when loaded with Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCsx68730

  Symptoms: Pseudowire switching configured between ASBR routers does not work and tracebacks are seen.

  Conditions: Occurs when Cisco 7200 router is used as Autonomous System Border Router (ASBR) and pseudowire switching is configured.

  Workaround: There is no workaround.

- CSCsy03568

  Symptoms: Spoke-to-spoke TCP applications fail over a GRE/IPSec tunnel on a hub and spoke scenario, when traffic flows through the hub.

  Conditions: The symptom is observed with the following conditions:

  - GRE/IPSec configured with crypto maps.
  - Hub has “ip tcp adjust-mss” configured under the tunnel interface that is facing the spoke from where traffic is coming.

  Workaround: Use tunnel protection instead of crypto maps.

  Alternate workaround: Disable CEF globally on hub (this may impact performance, so should be used with care).

- 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.

- CSCsy29533

  Symptoms: A T.38 fax relay call may fail.

  Conditions: The symptom is observed with an MGCP-controlled T.38 fax relay call when the gateway is configured for CA control T.38. The output of the **debug voip vtsp all** command shows fax relay as “DISABLED.”

  Workaround: Use Cisco IOS Release 12.4(15)T7 or Release 12.4(22)T.

- CSCsy45838

  Symptoms: The **show ip ospf border-router** command may cause a router to crash.

  Conditions: Occurs if the border table is recalculated in a significant way while the output is being printed on the console. The risk of a crash is reduced if you avoid using the auto-more feature and allow the entire output to display at once.

  Workaround: There is no workaround.

- CSCsy55821

  Symptoms: With a VTI tunnel between a Cisco ASR 1000 and another device (non-ASR), the VPN peer of a Cisco ASR 1000 is reporting packets with an invalid SPI.

Conditions: The symptom is observed in the following scenario:

- LAN-to-LAN VPN with VTIs.
- One VPN end point is a Cisco ASR 1002 (RP1) that is running Cisco IOS Release 12.2(33)XNC.
- The other VPN end point is a Cisco 7206VXR (NPE-G1) that is running Cisco IOS Release 12.4(15)T1 initially, then is upgraded to Cisco IOS Release 12.4(22)T and NPE-G2 plus VSA.

Workaround: There is no workaround.

Further Problem Description: At rekey, the Cisco ASR 1000 is sending delete-notify to the Cisco 7200 series router but still keeps using the old SA to encrypt, causing the drops.

- CSCsy56016

  Symptoms: BERT errors and jitter buffer errors reported on AS5xxx when using the **show tech** command.

  Conditions: The symptom is observed on the gateway when the **show tech** or **show as5400** commands are executed.

  Workaround: There is no workaround.

- CSCsz05181

  Symptoms: A router may reload unexpectedly.

  Conditions: The symptom is observed when the router has Bidirectional Forwarding Detection (BFD) configured and is actively sending keepalives. The crash has multiple possible triggers:

  - It can be triggered by certain show commands (**show bootvar** and **show c7200** are known to cause the problem). The issue will not be seen on every invocation of the commands. It is a rare timing condition, so the probability of the crash increases as the commands are run more frequently.
  - It can also be triggered by large scale BFD deployments (hundreds of sessions on a single router).

  Workaround: Unconfigure BFD.

- CSCsz31940

  Symptoms: Active secure NAT (SNAT) continuously prints the following tracebacks and the router is not operational while tracebacks are printed:

  ```
  %SYS-2-INSCHED: suspend within scheduler -Process= "<interrupt level>", ipl= 1,
  -Traceback= 0x41732A78 0x4009B8AC 0x42DF1EC8 0x41F780E4 0x41F9E790 0x41F53274
  0x41F7D830 0x400ECDD8 0x40069574 0x439BE7A8 0x439BC010 0x40047734 0x4000FCC0
  ```

  Conditions: The symptom is observed when flow switching and SNAT are configured on the router interface and SNAT traffic passes through the router.

  Workaround: Stop the SNAT traffic and wait for the tracebacks to clear.

- CSCsz45539

  Symptoms: Unable to attach the frame relay DLCI to the serial subinterface. The following error is received:

  ```
  %PVC already assigned to interface Serial3/0
  ```

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

  Workaround: There is no workaround.

- CSCsz48614

  Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCsz50423

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

  Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(24.6)T8.

  Workaround: There is no workaround.

- CSCsz56382

  Symptoms: The Tunnel0 interface used on a DMVPN hub is reporting “Tunnel0 is reset, line protocol is down” or no traffic is passing through this interface anymore.

  The IKE and IPSec SAs may still be up, but only the decaps counters will be seen increasing, not the encaps counters.

  Conditions: This symptom is observed on Cisco 2821 routers that are running Cisco IOS Releases 12.4(9)T7 or 12.4(15)T9. Other platforms and releases may be affected.

  Workaround: Shutdown Tunnel0 and create interface Tunnel1 with the same configuration instead, if you cannot reload the router.

  Otherwise reloading the router will resolve the issue. Do not configure another identical Tunnel interface in this case or you will run into CSCsl87438. If you reload the router at a later time, be sure to remove the duplicate Tunnel interface prior to the reboot.

- CSCsz62974

  Symptoms: Router crashes while querying for cvpdnTemplateActiveSessions.

  Conditions: Occurs if the vpdn-template name is long.

  Workaround: There is no workaround.

- 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.

- CSCsz72138

  Symptoms: A POS interface on a PA-POS-2OC3 may experience a stuck issue. All packets will be dropped after hitting the stuck scenario:

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
72048413<<<<<<<<<<<<<<<<<<<<All packets are getting dropped.
Queueing strategy: Class-based queueing Output queue:
197/1000/0 (size/max total/drops)<<<<<<<<<<<Output queue remains stuck at 197.
```

Conditions: This issue is common to different platforms such as the Cisco 7300, Cisco 7304, and Cisco 7200. Stuck can happen with and without service policy also.

Workaround:

1. Do a “shut/no shut” of the affected interface.

2. Do a soft OIR of the affected slot.

- CSCsz72591

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

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

  Workaround: There is no workaround.

- CSCsz76616

  Symptoms: PPP negotiation does not occur.

  Conditions: The symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 12.4(22)T2.

  Workaround: There is no workaround.

- CSCsz97833

  Symptoms: HTTP-based certificate revocation list (CRL) checking fails.

  Conditions: Occurs due to an extra character appended to the URL.

  Workaround: Disable CRL checking.

- CSCta02460

  Symptoms: On a router that has a PRI trunk towards the PSTN, you may hear dead air when calling any ISDN device that returns cause code 0x8484 in a PROGRESS message that also contains a progress_ind with value 8.

  Conditions: The symptom is seen when using the primary-4ess (PRI 4ESS) and primary-5ess (PRI 5ESS) switch type.

  Workaround: There is no workaround.

  Further Problem Description: The problem was discovered when a user attempted to call a cell phone on a wireless network that was switched off. The user did not have voicemail, and the wireless network played a message in the band to alert that the phone was off. It is this message that should be heard - but it is not, due to this bug.

  The issue is due to an invalid cause value sent from the provider for an outgoing to call to a mobile phone which is switched off. The cause value of 4 is not supported by PRI 4ESS switches. Hence ISDN will send a STATUS message reporting invalid information element contents and the provider disconnects the call.

- CSCta07104

  Symptoms: The **mpls bgp forwarding** command is not synced to the standby router.

  Conditions: When the **mpls bgp forwarding** command is not configured manually on the ASBR router, when eBGP Inter-AS session comes up, the command is auto-generated on the interface. The command is not synced to the standby router.

  Workaround: The issue will not be seen:

  1) When the **mpls bgp forwarding** command is configured manually.

  2) When the command is not configured manually, after a switchover, both the active router and the standby router will get that command.

- CSCta10075

  Symptoms: An incorrect logic in doing increment comparisons for counters, such as interface resets, will cause an EEM policy to be triggered. That is, if there are any numbers in the interface resets counter and a **clear counters** command is performed, on the next EEM poll interval the command executes, which is not correct.

  Conditions: This symptom is observed in the latest 12.4(24)T Cisco IOS release. Most of the newer 12.4T images are also affected.

  Workaround: There is no workaround.

- 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.

- CSCta20040

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

  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://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.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://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  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

  Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCta24037

  Symptoms: A Cisco router may reload due to a bus error and show the following messages:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 10:09:03 PDT Tue Sep 1 2009 addr=0x0,
  pc=0x4159DB10z , ra=0xFFFFB4DFz , sp=0x4F059900
  %ALIGN-1-FATAL: Illegal access to a low address 10:09:03 PDT Tue Sep 1 2009 addr=0x0,
  pc=0x4159DB10z , ra=0xFFFFB4DFz , sp=0x4F059900
  TLB (store) exception, CPU signal 10, PC = 0x415A2630
  ```

  Conditions: The symptom is observed on a Cisco 2851 router that is running Cisco IOS Release 12.4(24)T1.

  Workaround: There is no workaround.

- CSCta45976

  Symptoms: A BFD session cannot be established to the peer if the same IP address is configured on the device in a different VRF.

  Conditions: The symptom is observed when BFD sessions stay in a down state.

  Workaround: Remove the locally-configured IP address.

- 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.

- 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.

- 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.

- CSCta75923

  Symptoms: One-way voice may occur after a transfer through a CMM transcoder if the stream goes through an RTP-aware firewall such as an ASA. The transcoder in some transfer situations will reuse a previous SSRC, which causes a security violation.

  Conditions: In a situation where there are 3 SSRCs in a single transfer, the outgoing stream from the transcoder will reuse the first SSRC in place of the third SSRC. This is against the RTP RFC, and some firewalls may drop the packet. Some gateways and endpoints may also not correctly process the packets, depending on the strictness of the RFC implemented.

Workaround: It was found that some endpoints, like the Cisco Unified IP Phone 7960, activated a transfer with only 2 SSRC changes. It was also found that a Cisco Unified IP Phone 7941 with firmware 8-3-2 had the problem, but the latest 8-4-X image did not. Some endpoints, such as an autoattendant, do not have the ability to change this behavior. The only other workaround is to use a different type of transcoder than the ACT CMM.

- CSCta77678

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

- CSCta79428

  Symptoms: A call will not be connected for an EO-to-EO video call in Cisco UBE.

  Conditions: This symptom is observed when a SIP-to-SIP video call is started with an early offer.

  Workaround: There is no workaround.

- CSCta85026

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

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

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

  Workaround: There is no workaround.

- CSCtb13546

  Symptoms: A Cisco IOS router crashes with a bus error.

  Conditions: This symptom occurs when a Cisco IOS router is performing multihop VPDN (also known as tunnel switching). The router may infrequently crash due to a bus error.

  This crash is limited to cases where at least one of the following VPDN group commands are configured:

  ip pmtu ip tos reflect

  Workaround: Disable the above mentioned commands. However the consequences of this on user traffic must be evaluated first.

- CSCtb16459

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

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

Workaround: There is no workaround.

- 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.

- CSCtb25549

  Symptoms: Router crashes.

  Conditions: The symptom is observed with the following sequence:

  1. Use the **debug condition username** command.

  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.

- CSCtb26955

  Symptoms: The following error message is seen:

  ```
  %CRYPTO-4-GM_REGSTER_IF_DOWN: Can't start GDOI registration as interface
  FastEthernet1.2 is down
  ```

  Problem: The interface is not actually down. The registration should go through.

  Conditions:

  1) Manually clear the rekey SA (**clear cry isakmp** *connid*).

  2) Wait for the re-registration to start.

  Workaround: Use the **clear cry gdoi** *group* command or remove and add the crytpo map. The manual deleting of rekey SAs is not a valid option.

  Further Problem Description: An incomplete check in the code interprets this as "the associated interface is down." The registration fails with the GM_REGSTER_IF_DOWN error message.

- CSCtb29256

  Symptoms: A router crashes after entering the **sh isdn history** command.

  Conditions: This issue is seen in a Cisco 7206VXR (NPE-G2) that is running Cisco IOS Release 12.4(15)T9.

  Workaround: Avoid using the **sh isdn history** command and use the **sh isdn active** command.

- CSCtb34920

  Symptoms: Calls may intermittently be dropped or disconnected.

The debug output for “debug isdn q931” will reveal that the gateway is sending a Q.931 INFORMATION message similar to the following:

```
ISDN Se0/2/1:23 Q931: TX -> INFORMATION pd = 8 callref = 0x80AE
```

The connected service provider switch may respond with a Q.931 STATUS message similar to the following:

```
ISDN Se0/2/1:23 Q931: RX <- STATUS pd = 8 callref = 0x00AE Cause i = 0x81E17B -
Message type not implemented Call State i = 0x0A
```

The connected service provider switch may also respond with a Q.931 DISCONNECT message similar to the following:

```
ISDN Se0/2/1:23 Q931: RX <- DISCONNECT pd = 8 callref = 0x00AE Cause i = 0x81E4 -
Invalid information element contents
```

Conditions: This problem may occur when an ISDN PRI is configured to use “switch-type primary-4ess” or “switch-type primary-5ess.”

This problem may occur when an IP phone user blind transfers a call to another destination (another IP phone, IVR, IPCC queue, etc). The transfer request triggers the Cisco Unified Communications Manager (CUCM) server to send an H.225 INFORMATION message with a Signal IE to the Cisco IOS H.323 gateway indicating to start/stop playing ringback tone toward the PSTN. The Cisco IOS H.323 gateway should generate the ringback tone, but it should NOT send the Q.931 INFORMATION message toward the connected service provider switch.

The 4ess spec indicates that the INFORMATION message is NOT supported per AT&T TR 41459 section 3.1.8. Also the Lucent AT&T 235-900-342 5ess spec does not even mention the INFORMATION message in section 4.2 which covers all other supported Q.931 message types.

Workaround: Another similar defect CSCsr38561 was previously opened for this same type of problem with “switch-type primary-ni” and has now been resolved.

If you are running a version of Cisco IOS, which has the fix for CSCsr3856, it may be possible to reconfigure the Cisco IOS gateway user side of the PRI to use “switch-type primary-ni” even though the connected service provider switch may be provisioned for 4ess or 5ess. This should only be used as a temporary workaround because it could expose other interworking errors due to switch-type mismatch configuration.

- CSCtb37673

  Symptoms: Using a break action within a programmatic Embedded Event Manager applet causes the policy to exit.

  Conditions: The symptom is observed when a break action is executed within a loop. For example:

  action 001 foreach line $output "
  " action 002 if $line eq "" action 003 break action 004 end action 005 puts “Made it here”

  After the break is executed, the policy aborts. The “Made it here” string is not printed.

  Workaround: If possible, use “if ... goto” statements to get out of the loop without calling break. For example:

  action 001 foreach line $output "
  " action 002 if $line eq "" goto 004 action 003 end action 004 puts "Made it here"

- 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.

- 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.

- CSCtb57180

  Symptoms: A router may crash with a software-forced crash.

  Conditions: Under certain conditions, multiple parallel executions of the **show users** command will cause the device to reload.

  Workaround: It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted devices to connect to the device via telnet, reverse telnet, and SSH.

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

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

  The following example permits access to VTYs from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from everywhere else:

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 permit host 172.16.1.2
Router(config)# line vty 0 4
Router(config-line)# access-class 1 in
```

  For devices that act as a terminal server, to apply the access class to reverse telnet ports, the access list must be configured for the aux port and terminal lines as well:

```
Router(config)# line 1 <x>
Router(config-line)# access-class 1 in
```

  Different Cisco platforms support different numbers of terminal lines. Check your device's configuration to determine the correct number of terminal lines for your platform.

  Setting the access list for VTY access can help reduce the occurrences of the issue, but it cannot completely avoid the stale VTY access issue. Besides applying the access list, the following is also suggested:

  1. Avoid nested VTY access. For example, RouterA->RouterB->RouterA->RouterB.

  2. Avoid issuing the **clear vty** command or the **clear line** command when there is any nested VTY access.

  3. Avoid issuing the **clear vty** command or the **clear line** command when there are multiple VTY accesses from the same host.

  4. Avoid issuing the **clear vty** command or the **clear line** command when router CPU utilization is high.

  5. Avoid issuing the **show users** command repetitively in a short period of time.

  Again, the above can help reduce the occurrences of the issue, but it cannot completely avoid the issue.

- 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.

- CSCtb60330

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

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

  Workaround: Disable DPDs.

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

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

  debug crypto isakmp
  debug crypto ipsec
  debug crypto kmi

  The following entry can be seen in debugs:

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

- CSCtb66925

  Symptoms: A router may crash during a port scan to TCP port 53.

  Conditions: DNS functionality must be configured on the device.

  This crash has been observed only in 12.4(24)T, 12.4(24)T1, and 12.4(22)T. It is a timing condition on processing DNS TCP traffic.

  Workaround: Create an ACL to deny traffic to the device on TCP port 53:

  The following mitigations have been identified for this Cisco bug ID, which may help protect an infrastructure until an upgrade to a fixed version of Cisco IOS software can be scheduled:

  * Infrastructure Access Control Lists (iACLs)

  Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for these specific vulnerabilities. The iACL example below should be included as part of the deployed infrastructure access list, which will protect all devices with IP addresses in the infrastructure IP address range:

  ```
  !---
  !--- Feature: DNS over TCP
  !---
  access-list 150 permit tcp TRUSTED_HOSTS WILDCARD
     INFRASTRUCTURE_ADDRESSES WILDCARD eq 53
  !---
  !--- Deny DNS TCP traffic from all other sources destined
  !--- to infrastructure addresses.
  ```

```
!---
access-list 150 deny tcp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 53
!---
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.
!---
access-list 150 permit ip any any
!---
!--- Apply access list to all interfaces (only one example
!--- shown).
!---
interface serial 2/0
 ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

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

* Receive ACLs (rACLs)

For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the Cisco 12000, 12.0(24)S for the Cisco 7500, and 12.0(31)S for the Cisco 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor.

Receive ACLs are designed to protect only the device on which they are configured. On the Cisco 12000, 7500, and 10720, transit traffic is never affected by a Receive ACL. Because of this, the destination IP address “any” used in the example ACL entries below refer only to the router’s own physical or virtual IP addresses. Receive ACLs are considered a network security best practice and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

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

- 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".

- 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.

- 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.

- 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.

- 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.

- 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 **debug webvpn sdps** command 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.

- CSCtc04228

  Symptoms: The **mgcp behavior g729-variants static-pt** command is the default and will show up in the configuration. This causes a problem when you save the configuration and downgrade to an earlier Cisco IOS release where this behavior is not present. There, the command will now be enabled when it was not 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.

- 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.

- 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.

- 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.

- CSCtc68705

  Symptoms: A router may crash with a bus error.

  Conditions: This symptom is observed when a Cisco firewall withdraws a default route and the Cisco IOS router has another default route as a backup. This symptom is observed only when peering with a firewall, not a Cisco IOS router.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCtd60858

  Symptoms: While testing dot1x accounting, spurious accesses are seen.

  Conditions: This symptom is observed while verifying the attributes in Access-Request, Access-Challenge, and Access-Accept packets.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(22)T3

Cisco IOS Release 12.4(22)T3 is a rebuild release for Cisco IOS Release 12.4(22)T. The caveats in this section are resolved in Cisco IOS Release 12.4(22)T3 but may be open in previous Cisco IOS releases.

- CSCej33698

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

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

  Workaround: There is no workaround.

- CSCsd77560

  Symptoms: SNMPv3 “auth” and “priv” users are lost across reload.

  Conditions: Occurs after a reload.

  Workaround: There is no workaround.

- CSCsg00102

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

  Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed.

  This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix CSCso04657 and CSCsg00102.

- CSCsk80396

  Symptoms: Router crashes when jitter operation takes place.

  Conditions: This crash is inconsistent and is seen while auto Ethernet operation is configured to carry on jitter operation on an interface configured with **no ethernet cfm enable**.

  Workaround: There is no workaround.

- CSCsl15443

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

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

Workaround: There is no workaround.

- CSCso05336

  Symptoms: A Cisco 1811 router reloads when trying to connect to irc.freenode.net during the first 36 hours following a reload.

  Conditions: The symptom is observed only in the first 36 hours following a reload.

  Workaround: Do not connect to irc.freenode.net the first 36 hours following a reload.

- CSCsq58289

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

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

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

- CSCsr16147

  Symptoms: Session is not getting disconnected when the locally configured timers expire.

  Conditions: Occurs while testing an internal build of Cisco IOS Release 12.4(22)T on the Cisco 7200.

  Workaround: There is no workaround.

- CSCsr96084

  Symptoms: A router crashes with the following error:

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

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

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

  ```
  interface Tunnel97 ... tunnel source POS6/0 ...
  interface POS6/0 ip address 10.2.0.1 255.255.255.252
  ip local policy route-map Force-GRE
  ip access-list extended Force-GRE permit gre host 10.2.0.1 any
  route-map Force-GRE permit 10 match ip address Force-GRE set interface POS6/0
  ```

- CSCsu32452

  Symptoms: Spurious memory access occurs.

  Conditions: Occurs while attempting to unconfigure the EzVPN client configuration on an EzVPN client inbound interface.

  Workaround: There is no workaround.

- CSCsv17698

  Symptoms: Packets may be incorrectly classified under child and parent classes.

Conditions: The symptom is observed when a two or three-level policy is configured/reconfigured coupled with the command **clear counters**. The symptom also occurs if a second level policy-map is detached and then re-attached to a grandparent policy. Some of the packets go through the intended parent (or grandparent) class and incorrectly go through the default class or no class at all of the child policy.

The issue is seen with a Cisco 7200 series router that is running Cisco IOS Release 12.4(20)T2, 12.4(22)T2 or 12.4(24)T.

Workaround: Reload the router. In some cases, unconfiguring and reconfiguring the policies will work.

- CSCsv65867

  Symptoms: NM-CEM-4SER modules installed in Cisco 3845 routers will not use network clock if one is available. Instead, they will use the local oscillator. This can be observed by using the **show cem** *slot/port/0* command.

  Conditions: This behavior is observed on a NM-CEM-4SER module installed in Cisco 3845 routers running Cisco IOS Release 12.4(20)T or later.

  Workaround: Use adaptive clocking to improve clock accuracy.

- CSCsw52277

  Symptoms: The previous primary crashes.

  Conditions: Occurs when a fresh Key Server with higher priority comes up and election is triggered.

  Workaround: There is no workaround.

- CSCsw67252

  Symptoms: When RTP-NTE and T.38 are both enabled, the re-invite for T.38 incorrectly includes Session Description Protocol (SDP) with RTP-NTE.

  Conditions: Occurs when both RTP-NTE and T.38 are enabled.

  Workaround: There is no workaround.

- CSCsx32283

  Symptoms: Router is crashes.

  Conditions: Occurs because of malformed LDAP packet.

  Workaround: There is no workaround.

- CSCsx42261

  Symptoms: Memory leak occurs with “CCSIP_SPI_CONTROL” process.

  Conditions: The error is found on a Cisco 3825 running the c3845-spservicesk9-mz.124-20.T1.bin image and using Skinny Call Control Protocol.

  Workaround: There is no workaround. Reload the router.

- CSCsx55861

  Symptoms: On a Cisco 880 router, the UUT crashes when the PVC comes up and when “auto qos voip” is configured.

  Conditions: The symptom is observed when “auto qos voip” is configured under ATM and when the PVC is toggled (due to, for example, a shut/no shut of the ATM interface or a cable being pulled and then restored).

  Workaround: There is no workaround.

- CSCsx56837

  Symptoms: Intermittent one-way audio occurs during a call.

  Conditions: Calls through a Cisco IOS transcoding device may experience one-way audio when certain signaling RTP payload types are received.

  Cisco IOS VoIP gateways utilize named signaling events (NSE) to signal certain transitions to other states for active calls. Modem passthrough is a feature by which two gateways can upspeed to g711 an active RTP session. This is signaled through the use of certain NSE packets between these devices.

  Modem passthrough using NSE through a transcoding session is not supported. However, under some situations on a voice call (no modems on the call), it is possible that the modem detection algorithm on the DSP may falsely detect a modem signal. If this occurs, a NSE will be sent out if modem passthrough is configured on the VoIP gateway. If the transcoder session that is bridging the two calls between the VoIP gateways receives this NSE packet, all further processing of RTP packets will stop in that direction.

  Workaround: Disable modem passthrough on the end VoIP gateways.

- CSCsx67255

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

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

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

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

  Workaround:

  1. Reload the router to clear the channel. If a reload cannot be done, busy out the channel with the failed calls using the **isdn busy b_channel** command under the serial interface.
  2. If this issue is due to oversubscription of the DSP resources, change the configuration to meet the DSP resources available on the gateway. Further information can be found with the CCO “DSP Calculator” at http://www.cisco.com/web/applicat/dsprecal/dsp_calc.html.
  3. If the issue is related to timing issues upon reload, shutdown the voice-port in question before reloading the gateway. When the gateway comes back up, take the voice-port out of shutdown.

- CSCsx68596

  Symptoms: The system may display a %SYS-3-NOELEMENT message, similar to:

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

  after which system behavior can be unpredictable. If the interrupts are rapid enough, the system may become unresponsive (hang), use all available memory to create more buffer elements, or crash due to CSCsj60426.

  Conditions: The message is caused by extremely rapid changes in flow control or modem control lead status on a console port.

Workaround: Eliminate the source of the rapid lead changes. As modem control and flow control are generally not supported on the console, these changes are usually due to misconfigured devices attached to the console.

- CSCsx75353

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

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

  Workaround: Remove the AIM compression card from the motherboard.

- CSCsx95906

  Symptoms: Call fails when Nortel endpoint is at remote end.

  Conditions: Nortel endpoint sends a long contact header field value, which exceeds the maximum limit of the Cisco device. This remote contact overwrites memory for the from header and results in a dialog mismatch from the new message generated by the gateway.

  Workaround: There is no workaround.

- CSCsy05111

  Symptoms: A router crashes after enabling and disabling NBAR on an interface if a class-map with match protocol is configured first (“match protocol rtp audio”).

  Conditions: The symptom is observed if the “match protocol rtp audio” statement is found in the class-map configuration. RTP uses a label heuristic which quickly reproduces the bug.

  Workaround: Do a config/no-config on one interface while keeping NBAR configured on any other interface.

- CSCsy06128

  Symptoms: When a router is about to renew a certificate, the following syslog message is seen

  `"%PKI-6-CERTRENEWAUTO: Renewing the router certificate for trustpoint xxx".`
  However, no certificate is received until a few hours later.

  Conditions: The issue only happens on a Cisco 871 running Cisco IOS Release 12.4(15)T8 and 12.4(22)T1 or earlier releases. This issue is only seen with a very short certificate lifetime, such as 1 hour.

  Workaround: Increase the certificate lifetime to a few days or more.

- CSCsy10893

  Symptoms: A router reloads occasionally after the command **show buffers leak** is repeatedly issued.

  Conditions: The symptom is observed when issuing 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.

- CSCsy16078

  Symptoms: A GETVPN group member might reload when removing “crypto map” from the interface, if that crypto map also contains a dynamic-map set together with the GDOI set.

  Conditions: The symptom only occurs when a dynamic-map set is added to a crypto map that is already applied to an interface and then the whole crypto map is removed, added and removed again. It is on the second removal that the reload occurs.

  Workaround: Execute the command **clear crypto gdoi** before removing the crypto map from the interface.

- CSCsy16177

  Symptoms: Cisco 2811 experiences invalid checksum over SCP on SSH version 2.

  Conditions: Occurs on a Cisco 2811 with flash type file system.

  Workaround: There is no workaround.

- CSCsy22311

  Symptoms: Using secure copy (SCP) between Cisco routers may cause compatibility issues.

  Conditions: Occurs when using SCP SSH version 2 between a Cisco 1800 and Cisco 2800.

  Workaround: There is no workaround.

- CSCsy24266

  Symptoms: A call from a night hunt forwarded to BACD dial by an extension to an ephone (call forwarding no answer) to voicemail goes to the night hunt number and not the last redirected number.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsy29940

  Symptoms: Unable to configure inspect for any protocol in self zone.

  Conditions: Occurs when configuring class-map with match protocol and trying to attach to self-zone pair.

  Workaround: The issue is not seen when **match access-group** is used.

- CSCsy31552

  Symptoms: A Cisco 1841 router equipped with xDSL WIC will suddenly stop forwarding packets. The packets will appear as output drops on the ATM interface statistics. Under the PVC level, there are no drops. The DSL line is not flapping but the ATM interface(s) report output drops.

  Conditions: The symptom is observed when using a Cisco 1800 and 2800 series router equipped with the same ADSL-WIC module. The ATM interface(s) need to be bridge-group configured. The bridge-group is in forwarding mode.

  Workaround: Reload the router.

- CSCsy39667

  Symptoms: On a PPP aggregator using dhcp-proxy-client functionality, in a situation where a PPP client session is torn down and then renegotiated within 5 seconds, the DHCP proxy client may send a DHCP RELEASE for the previous DHCP handle after the new DHCP handle (created as a result of new IPCP CONFREQ Address 0.0.0.0) has accepted the same IP address allocation from the offnet DHCP Server. This results in the offnet DHCP server having no record of the lease as it exists on the PPP aggregator which causes future addressing conflicts.

  Conditions: The symptom is observed on a Cisco 7200 (NPE-400) and 7200 (NPE-G2) that is running Cisco IOS Release 12.4 T, or 12.2 SB.

  Workaround:

  1. Automated: Write a script to compare active leases on the PPP aggregator to active leases on DHCP server. If a lease is found to only exist on the PPP aggregator, use **clear interface virtual-access** to recover.
  2. Manual: use the command **clear interface virtual-access**.

Further Problem Description: This issue occurs because the DHCP client holdtime is static at 5 seconds and there are no IOS hooks to tie PPP LCP session removal and IPAM to suppress stale DHCPRELEASES waiting in queue for HOLDTIME to expire.

- CSCsy40285

  Symptoms: Cisco 3845 crashes during end point registration.

  Conditions: Occurs on a router running the c3845-adventerprisek9-mz.124-24.T.bin image.

  Workaround: Increase **tcp idle-timeout** to 7200 seconds.

- CSCsy40745

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

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

  Workaround: Do not configure alternate SSH ports.

- CSCsy42401

  Symptoms: User group class matching fails when NAT is turned on.

  Conditions: The symptom is observed with IOS FW user group inter-operated with NAT.

  Workaround: There is no workaround.

- CSCsy43875

  Symptoms: A system may crash due to “Watchdog Time Expired” errors during normal operation without generating a crashinfo file or error messages prior to the crash.

  Conditions: The symptom is observed when any code tries to generate traceback via trace_caller. It is more likely to occur if BFD is configured.

  Workaround: There is no workaround.

- CSCsy46007

  Symptoms: EzVPN tunnel will not come up after a reload. EzVPN is trying to connect to the peer with outside interface IP address to be “NULL”. The below debug message will be seen if “debug crypto isakmp” is enabled:

  ```
  EX: "ISAKMP:(0):receive null address from sa_req (local 0.0.0.0, remote 192.168.76.40)
  ```

  Conditions:

  1. EzVPN is in connect acl or auto mode
  2. Outside interface is configured on dialer interface.
  3. This issue is seen only when EzVPN is trying to ask the dialer to kick start and dialer is not yet ready or dialer has not yet assigned the IP address to the interface.

  Workaround: There is no workaround.

- CSCsy48838

  Symptoms: A router may crash with the following (or similar) message:

  %ALIGN-1-FATAL: Corrupted program counter

  Conditions: The symptom is observed when IOS firewall/ip inspect on H323 traffic is configured (“ip inspect name MY_INSPECT h323”).

  Workaround: Do not inspect H323.

- CSCsy52077

  Symptoms: Call passing through a Cisco Unified Border Element (CUBE) is dropped after more than 1 hour.

Conditions: Occurs when there are multiple point-to-point calls going through CUBE at same time.

Workaround: There is no workaround.

- CSCsy57750

  Symptoms: IPIPGW reloads while making an RSVP-enabled voice call with media statistics configuration.

  Conditions: The symptom is observed with Cisco IOS 12.4(24.6)T2 image.

  Workaround: There is no workaround.

- CSCsy58450

  Symptoms: Zone based firewall drops packets that pass through a VPN tunnel (both forward and reverse traffic). The drops are usually seen for UDP traffic. The following traceback may be seen:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
  ```

  Conditions: Occurs when firewall is configured with crypto-map tunnels. Cisco IOS Release 12.4(20)T2 and 12.4(22)T and earlier releases are not affected.

  Workaround: Change the UDP timeout to a reasonably larger value. The default value is 30 seconds, and changing it to something like 300 seconds has been found to make a difference. To do this

  1. Create an “inspect” parameter map with any name if it does not exist, then add the new UDP idle timeout.

     parameter-map type inspect <param-map-name> udp idle-time 300

  2. Attach the parameter map to all the inspect actions. **policy-map type inspect <policy-name> class type inspect <class-name> inspect <param-map-name>**

- CSCsy69681

  Symptoms: Policy-based routing (PBR) fails to resolve next-hop.

  Conditions: Occurs when PBR is configured on a Cisco 871 to forward traffic to a DHCP-enabled interface.

  Workaround: There is no workaround.

- CSCsy73123

  Symptoms: Connected route on port-channel sub-interface is not removed when port-channel is down.

  Conditions: Happens when using /22 subnet. Does not happen when using /24 subnet.

  Workaround: There is no workaround.

- CSCsy73981

  Symptoms: Cisco AS5400 shows memory leak for DSMP, VTSP, and MGCP processes. Occurs about once a month.

  Conditions: After some time, the memory leak symptoms are seen on the gateway, although normal operations are not affected. Eventually all memory is consumed, and the gateway hangs. Only a manual reboot can bring it back to service.

  Workaround: There is no workaround.

- CSCsy79955

  Symptoms: Reverse SSH using PVDM2 modems fails. If the **ssh -l <username>:<line #> <ip>** command is entered, modem activation is triggered. The input of “atdt<number>” is making it to the modem, meaning whatever the <number> field is typed, it is reported in the debugs. However, the modem does not send anything back to router about it and no connection is made. At modem prompt, “at”, “at&f”, “ate1” (and perhaps others) do not appear to be taken.

  Conditions: Seen on routers running Cisco IOS Release 12.4(22)T and 12.4(23). Appears to be issue with all releases. Issue is seen when using both **ssh -l <username>:<line #> <ip>** and by using SSH from a client to a particular line.

  Workaround: There is no workaround.

- CSCsy84474

  Symptoms: In an H323 IP-to-IP Gateway (IPIPGW), during call setup when the OLC-ACK is received after the connect message, the call is not completed and the return OLC-ACK is not forwarded by the IPIPGW. The issue is sporadic and does not occur all the time.

  Conditions: This has been observed on a IPIPGW running Cisco IOS Release 12.4(20)T1-ES, having an H323 on both sides of the gateway. This only happens when the connect message is received before OLC-ACK exchange between the parties is complete.

  Workaround: There is no workaround.

- CSCsy88640

  Symptoms: A core dump may fail to write, with the following errors seen on the console:

  ```
  current memory block, bp = 0x4B5400A0,
  memorypool type is Exception
  data check, ptr = 0x4B5400D0
  bp->next(0x00000000) not in any mempool
  bp_prev(0x00000000) not in any mempool
  writing compressed ftp://10.0.0.1/testuncached_iomem_region.Z
  [Failed]
  writing compressed ftp://10.0.0.1/testiomem.Z
  [Failed]
  writing compressed ftp://10.0.0.1/test.Z
  [Failed]
  %No memory available
  ```

  Conditions: This is only seen for memory corruption crashes when “exception region-size” is configured to a value that is not divisible by 4.

  Workaround: The recommended setting for exception region-size is 262144 in newer images. In older images, where the maximum configurable value is 65536, use the maximum.

- CSCsz03260

  Symptoms: A gateway may take an exception when receiving an inbound H320 call when the call is placed via ISDN overlap sending.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(22)T1.

  Workaround: There is no workaround.

- CSCsz13123

  Symptoms: Frame-relay DLCI is not released from interface in a certain configuration sequence.

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS 12.4T images.

  Workaround: There is no workaround.

- CSCsz14236

  Symptoms: LLC stops forwarding I frames, but continues to respond to poll frames.

  Conditions: The symptom is detected when the output from **show llc** shows that frames are queued up for transmission in the Tx Queue. If DLSw is transporting the LLC frames, the associated DLSw circuit will show that the link is in a max congestion state.

  Workaround: There is no workaround.

- CSCsz20496

  Symptoms: A Cisco VG224 voice gateway displays the wrong secondary dialtone to the customer if “cptone CN” is configured under the voice-port.

  Conditions: The symptom is observed with Cisco IOS Releases 12.4(24)T, 12.4(20)T1, and 12.4(9)T7.

  Workaround: Upgrade to the latest IOS version (see bug CSCsk28301) and change the dial_tone2 to make it same as the dialtone by using the command **test voice tone cn 2nd_dialtone**:

```
event manager applet setCNsecondDialtone
  event syslog occurs 1 pattern ".*%SYS-5-RESTART: System restarted --.*"
  action 1.0 syslog msg "Setting DIAL_TONE2 for cptone CN"
  action 2.0 cli command "enable"
  action 3.0 cli command "test voice tone CN 2nd_dialtone 1 450 0 -100 -100 -100 0 0 0
0xFFFF 0 0 0 0 0 0 0"
  action 4.0 syslog msg "DIAL_TONE2 for cptone CN has been set"
```

  Copy the script to the running-configuration and then save it to NVRAM. If the router reloads, the setting “test voice tone CN 2nd_dialtone 1 450 0 -100 -100 -100 0 0 0 0xFFFF 0 0 0 0 0 0 0" will automatically be re-asserted. If you want the command set immediately without a reload then cut and paste the command directly at the EXEC prompt.

- CSCsz23976

  Symptoms: A Cisco 7200 series router that is running Cisco IOS Release 12.4(15)T7 may experience an unexpected reset while forwarding traffic with a Cisco 7200 VSA.

  Conditions: The symptom is observed on a Cisco 7200 series router running with a Cisco 7200 VSA installed on Cisco IOS 12.4(15)T code.

  Workaround: There is no workaround.

- CSCsz24327

  Symptoms: The following command crashes the router:

  demo-gm1(config)#int vlan 10

  demo-gm1(config-if)#no ip igmp join-group <group_address> source <src_addrs>

  Conditions: The problem happens when we do join and unjoin a particular source-group immediately. Also, the problem is seen only when the DNS server is configured for IGMP SSM group to source mapping is not responding. If the DNS responds properly, the problem may not occur. Also, if DNS server is not present.

  Workaround: Wait for 2 to 3 seconds after entering the **igmp join-group** command before unjoining the group. If the host has just booted, wait until the entire booting process is completed before unjoining the group.

- CSCsz29320

  Symptoms: A Cisco 3845 running Cisco IOS Release 12.4.(20)T2 reloaded due to software-forced crash while experiencing the following error:

```
%SYS-6-STACKLOW: Stack for process MGCP Application running low, 0/12000
%Software-forced reload
```

Conditions: The crash suggests that the issue is just one of inefficient stack usage.

Workaround: There is no workaround.

- CSCsz34920

  Symptoms: Router continuously reboots.

  Conditions: The symptom is observed when an NME-502 is installed in the router.

  Workaround: Replace or take out the NME-502.

- CSCsz36002

  Symptoms: GETVPN traffic stops. Upon entering **show crypto engine accelerator statistic**, you will see the 'ppq full' counter going up.

  Conditions: Occurs on a Cisco 3800 running Cisco IOS Release 12.4(22)T or 12.4(24)T.

  Workaround: Either reload the router or enter the following sequence of commands:

  ```
  configure terminal
  no crypto engine accelerator
  crypto engine accelerator
  ```

- CSCsz45567

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

- CSCsz45855

  Symptoms: Cisco Unified Border Element (CUBE) ignores reINVITEs from Cisco Customer Voice Portal (CVP).

  Conditions: While call transfer is in progress and CUBE is waiting for NOTIFY (with 200 or any final response code) after receiving NOTIFY (with 100), it receives INVITE.

  Workaround: There is no workaround.

- CSCsz48680

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled. Remote code execution may also be possible.

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

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

- CSCsz48914

  Symptoms: Next Hop Resolution Protocol (NHRP) registration and tunnels are not up between first- and second-level hubs.

  Conditions: Occurs in hierarchical topology.

  Workaround: There is no workaround.

- CSCsz49741

  Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCsz50275

  Symptoms: The firewall is configured to reset if an invalid command goes through the unit under test. But the reset action does not happen, and this functionality issue observed all inspected application traffic, such as IM, SIP, and P2P.

  Conditions: This problem occurs both when Cisco Common Classification Policy Language (C3PL) is used, and when it is not used.

  Workaround: There is no workaround.

- CSCsz56169

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

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

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

- CSCsz58785

  Symptoms: When using the Cisco Service Selection Gateway (SSG) feature in Cisco IOS Release 12.4(22)T with TCP-Redirect and SSG Port Bundle Host Key (PBHK)/port-map, redirected packets may be dropped and not be forwarded to the Cisco Subscriber Edge Services Manager (SESM).

  Conditions: Occurs on a router running Cisco IOS Release 12.4(22)T and configured for SSG and with “ssg port-map” and “ssg tcp-redirect” configured.

  Workaround: There is no workaround known other than using an older IOS release or disabling port-bundle host key (PBHK).

- CSCsz60659

  Symptoms: The cooperative GDOI keyserver starts printing %GDOI-5-COOP_KS_REACH and/or %GDOI-5-COOP_KS_UNREACH syslog messages.

  Conditions: The symptom is observed if two or more ISAKMP connection attempts fail, which might be normal in production networks.

  Workaround: There is no workaround.

  Further Problem Description: In fixed versions, the logic of the reachability test was changed to avoid this problem.

- CSCsz68373

  Symptoms: After configuring NAT, traffic fails to hit the policy-map of the frame-relay serial interface.

  Conditions: This issue is seen with NM-1T3/E3 of a Cisco 3845 router only when NAT is configured.

  Workaround: Remove and re-apply the frame-relay map-class under serial interface after NAT is configured.

- CSCsz70486

  Symptoms: On a Cisco 7200 series router with a VPN Services Adapter (VSA) installed, the outbound interface Access Control List (ACL) is not checked if a crypto map is applied to the interface and Cisco Express Forwarding (CEF) is enabled globally.

  Conditions:

  1. Egress ACL configured on the interface.
  2. A crypto map is applied to the same interface.
  3. VSA is installed in the chassis.
  4. CEF is enabled.

  Workaround: Remove the VSA or the crypto map, or disable CEF.

- CSCsz71392

  Symptoms: WCCP stops functioning when GDOI SA is accelerated by VSA.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(24)T with VSA (FPD 0.23). It is seen when **ip wccp** *61* **redirect out** and **ip wccp** *62* **redirect in** are applied to the inside interface, and traffic gets WCCP GRE redirected to WAE. When GDOI crypto-map (currently in inbound-only state) is applied to the outside interface, traffic is returned from WAE via WCCP and GRE gets dropped within UUT.

  Workaround: Disabling VSA with **no crypto engine slot 0** restores connectivity to normal.

- CSCsz74629

  Symptoms: There is a delay in the propagation of interface link down state. Link failure is detected with a huge delay once the other end of the link gets disconnected.

  Conditions: The symptom is observed on a Cisco 1861 router that is running Cisco IOS Release 12.4(24)T.

  Workaround: The default keepalive period is 10 seconds and the periodic function which updates the link state change runs on the order of keepalive time, hence it takes long time to detect the link down state. If keepalive is set to 1 or 2 seconds, the time taken to detect link down is normal.

- CSCsz75186

  Cisco IOS Software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause an affected device to reload or hang. The vulnerability may be triggered by a TCP segment containing crafted TCP options that is received during the TCP session establishment phase. In addition to specific, crafted TCP options, the device must have a special configuration to be affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability.

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

- CSCsz79901

  Symptoms: Firmware file download using the TR-069 Agent on a router fails.

Conditions: The symptom is observed when doing a firmware upgrade using the TR-069 Agent on a router and when the URL is given as “http://{ip address}/dir/filename.bin?{name}={value}”. This issue is noticed only with the TR-069/CWMP Agent.

Workaround: Firmware download works if the URL is given as “http://{ip address}/dir/filename.bin”.

- CSCsz81308

  Symptoms: Using ‘send break’ causes router to display ‘TLB Miss exception’ error and hang indefinitely.

  Conditions: Occurs on a Cisco 800 router running Cisco IOS Release 12.4(24.6)T9.

  Workaround: There is no workaround.

- CSCsz85919

  Symptoms: A router reloads with a SegV exception.

  Conditions: The symptom is observed with a router that is running Cisco IOS Release 12.4(20)T2 with both NAT and output ACLs configured. It occurs when the packet size changes due to NAT (this can happen with SIP/H.323 etc.).

  Workaround: There is no workaround.

- CSCsz86837

  Symptoms: After few days of normal operations, Cisco L2TP network server (LNS) starts rejecting significant percentage of L2TP sessions. While problem is present **debug vpdn l2x-event** shows:

  ```
  "312238: May 13 14:32:43.042: VPDN Tnl/Sn 0 0 CLIENT: fail to set server 000BA226 ->
  session 000BA226
  312239: May 13 14:32:43.042: VPDN Unknown vpdn syslog error due to AAA disconnect code
  0"
  ```

  Conditions: Occurs after a few days of LNS uptime.

  Workaround: There is no workaround.

- CSCsz89904

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled. Remote code execution may also be possible.

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

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

- CSCsz93207

  Symptoms: In an EZVPN scenario, the traffic to the internet is not getting NATed.

  Conditions: The symptom is observed in an EZVPN scenario with “identical addressing” and “split tunnel” configured.

  Workaround: Use Cisco IOS Release 12.4(15)T3.

- CSCsz96323

  Symptoms: A Cisco 7301 router crashes with “protocol pptp” configured.

  Conditions: The symptom is observed with a Cisco 7301 router when “protocol pptp” is configured.

  Workaround: There is no workaround.

- CSCta00794

  Symptoms: %SYS-3-CPUHOG is seen when multicast fanout performance test is executed with a large number of IGMP or PIM joins and forwarding out through a large number of OIF (1000 sub-interfaces).

  Conditions: Observed on a Cisco 7200 router running Cisco IOS Release 12.4(24.06)T9.

  Workaround: There is no workaround.

- CSCta02089

  Symptoms: There is a crash on a Cisco AS5400 due to CPU signal 10.

  Conditions: The symptom is observed on a Cisco router due to expiration of freed receive_digit timer in SIP

  Workaround: There is no workaround.

- CSCta04123

  Symptoms: A router may crash with a “STACKLOW” message or memory corruption.

  Conditions: The symptom is observed when the router is configured for IP inspect (only a basic IP inspect configuration is necessary).

  Workaround: Disable IP inspect.

- CSCta04391

  Symptoms: Router with dynamic NAT for unicast and multicast traffic crashes after deleting **ip nat inside source list**.

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

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

- CSCta05809

  Symptoms: A group member on a GETVPN network may stop passing encrypted traffic.

  Conditions: A GETVPN group member (GM) may accept and process an old or duplicate rekey message from the designated key server (KS). If the rekey message includes a TEK which was previously used to encrypt data, but which has already expired, the GM may become unable to send and receive encrypted traffic.

  Workaround: There is no workaround.

- CSCta07484

  Symptoms: A crash may occur on a CME when doing a web query on an ephone.

  Conditions: The symptom is observed when doing a web query on an ephone and maximum SIP phones are not configured on the CME under “voice register global”.

  Workaround: Configure maximum supported SIP phones under “voice register global”.

- CSCta28068

  Symptoms: The Citrix server (XenApp 5.0) cannot be accessed through WebVPN when using IE. The following message is shown:

  ```
  Cookies required
  This web site uses cookies in order to provide you with access to your published
  resources. You must configure your browser to accept cookies. Contact your system
  administrator for assistance.
  ```

  Conditions: The symptom is observed when using IE and XenApp 5.0.

Workaround: Use Firefox.

- CSCta35393

  Symptoms: CPE WAN Management Protocol (CWMP) agent on a Cisco Unified CallManager Express (CME) causes CPU to spike to 96%.

  Conditions: The symptom is observed when configuring the CWMP agent and placing a phone call.

  Workaround: Disable the CWMP agent.

- CSCta39579

  Symptoms: VPN routing/forwarding (VRF) Network Address Translation (NAT) is not translating UDP traffic at all. The inside local IP is still used after NAT. If the inside local IPs are not routable on the NAT outside side of the network this breaks all applications relying on UDP. ICMP and TCP traffic are not impacted

  Conditions: Occurs when NAT is inside a VRF. nat is in vrf

  Workaround: Make sure the inside local is known on the NAT outside side of the network.

- CSCta39763

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

  MJH-VG01# **show memory all totals**

  Allocator PC Summary for: Processor Displayed first 2048 Allocator PCs only

  PC Total Count Name 0x6010B9E8 9891336 513 ISDN Call Tabl

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

  Workaround: There is no workaround.

- CSCta43033

  Symptoms: Cisco Unified Border Element (CUBE) gives OLC reject during transfer despite correct codec negotiation. The cause code is 57.

  Conditions: Occurs under reasonable load and with many call transfers (such as CVP or IPCC environment).

  Workaround: There is no workaround.

- CSCta45116

  Symptoms: EAP-FAST authentication fails between router and client (PC or laptop running ADU).

  Conditions: The symptom is observed when the wireless client is running “ADUv2.x” and the router is running with Cisco IOS Release 12.4(15)T8.

  Workaround: Upgrade the wireless client ADU to version 3.x or 4.x.

- CSCta45845

  Symptoms: All show commands under crypto are showing blank outputs. For example **show crypto pki certificates** shows a blank output, even though there may be some crypto certificates on the device.

  Conditions: This happens only when using web interface to an IOS device. The commands are:

```
7200-12-3#sh crypto pki ? certificates
Show certificates counters
Show PKI Counters crls
Show Certificate Revocation Lists server S
how Certificate Server session
```

```
Show PKI Session Data timers
Show PKI Timers token
Show PKI Token(s) trustpoints Show trustpoints
```

Workaround: There is no workaround.

Further Problem Description: CCA uses HTTP(s) service to get the output. Even when the certificate is shown using telnet/SSH, CCA GUI shows as unconfigured.

- CSCta46486

  Symptoms: CPU hogging in IKE and traceback seen on headend router terminating large amount of DVTIs.

  Conditions: The symptom is observed with any kind of outage on the remote site or clearing large amount of tunnels with the headend router actively participating in the routing and re-distributing the routes learned via the tunnel to the central site.

  Workaround: There is no workaround.

- CSCta65793

  Symptoms: Router crashes while configuring “no auto-summary” in EIGRP at startup.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS 12.4M and 12.4T images.

  Workaround: As the router processes the auto-summary command prior to any interfaces participating in EIGRP becoming fully established, the workaround is to defer configuring the auto-summary command until after interfaces have been fully enabled and are participating in EIGRP.

- CSCta68917

  Symptoms: Cisco IOS allows duplicate installation of the same SSL VPN Client (SVC) packages with different sequence numbers.

  Conditions: Because of this defect, uninstallation of the SVC package causes an error when the same package has been installed more than once.

  Workaround: Install a SVC package only once on the router with the required sequence number.

- CSCta69118

  Symptoms: The ping from CE1 to CE2 fails when VLAN xconnect is provisioned, even though the session is up.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(20)T4.

  Workaround: There is no workaround.

- CSCta75271

  Symptoms: When we change a policy-map from a pure precedence policy (only match precedence classes) to a pure DSCP policy (only match DSCP classes), it causes a crash.

  Conditions: When we remove the last precedence/DSCP class from a pure policy and replace it with DSCP/QoS_group, it causes a crash. Occurs in Cisco IOS Release 12.4(20)T and 12.4(24)T throttles.

  Workaround: Remove the service-policy from the interface, then make the change to the policy-map and reapply the service-policy on the interface again.

- CSCta79634

  Symptoms: System crash in L2TP. Following this, most of the L2TP setups fail.

  Conditions: The symptom occurs at an L2TP control-plane event.

Workaround: Clear VPDN again or reload the router.

- CSCta91556

  Symptoms: Packets are getting SSS switched on the LAC towards LNS.

  Conditions: The symptom is observed when bringing up any PPPoE or PPPoA session.

  Workaround: There is no workaround.

- CSCtb14400

  Symptoms: Packets received from the virtual-access CE-facing interface are not CEF-switched into the MPLS cloud.

  Conditions: The symptom is observed on a MPLS/VPN PE router.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(22)T2

Cisco IOS Release 12.4(22)T2 is a rebuild release for Cisco IOS Release 12.4(22)T. The caveats in this section are resolved in Cisco IOS Release 12.4(22)T2 but may be open in previous Cisco IOS releases.

- CSCsi43340

  Symptoms: DSMP is not programming the DSP for supervisory tone while alerting tone is there, which leads to FXO disconnect supervision issue.

  Conditions: Occurs on routers running Cisco IOS Release 12.3(14)T and later releases.

  Workaround: Downgrade to Cisco IOS Release 12.3(11)T.

- CSCsj17977

  Symptoms: The GETVPN rekey fails. The following error message shows in the syslog:

  ```
  %GDOI-3-GM_NO_IPSEC_FLOWS: IPSec FLOW limit possibly reached
  ```

  The **show crypto engine connections flow** will show that all flows are used. For hardware-accelerated platforms, use the **show crypto eli** command to see how many Phase IIs are supported.

  Conditions: This problem is seen when the registration is not successful on a group member and then the flow IDs allocated for that incomplete registration are not cleaned up.

  Workaround: Reload the router, if all the flow IDs are leaked.

- CSCsj46707

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

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

  Workaround: There is no workaround.

- CSCsk43926

  Symptoms: High CPU usage may occur interrupt context on an RP, and spurious memory accesses may be generated when a route-map update is checked. You can verify this situation in the output of the **show align** command.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for BGP.

  Workaround: There is no workaround.

- CSCsk45399

  Symptoms: A device might crash when the QoS configuration is changed.

  Conditions: This symptom is observed on a device that has a QoS configuration.

  Workaround: There is no workaround.

- CSCsq24002

  Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml.

- CSCsr27727

  Symptoms: A Cisco Catalyst 6000 reports the following message and unexpectedly reloads:

  ```
  %SYS-2-ASSERTION_FAILED: Assertion failed: "wccp_acl_item_valid(item,NULL)"
  ```

  Conditions: This symptom is observed on a WS-C6509 that is running Cisco IOS Release 12.2(33)SXH2a.

  A WCCP service is configured with a redirect-list referring to a simple ACL.

  Workaround: Use an extended ACL as the WCCP redirect-list.

- CSCsr41631

  Symptoms: AnyConnect client is connecting to a Cisco ISR router that is running Cisco IOS Release 12.4(20)T with hardware encryption and CEF enabled. Client is unable to reach the inside interface IP address but can communicate with devices behind the router.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(20)T with hardware encryption and CEF enabled

  Workaround: Disable CEF globally and/or disable hardware encryption.

- CSCsr44382

  Symptoms: Add-on modules (7914/7915/7916) are not showing correct shared line status after registering.

  Conditions: This symptom occurs when the add-on module has a shared line configured on it, and the add-on module has just recently registered. The share line status on the add-on module is not updated after add-on registers.

  Workaround: There is no workaround.

- CSCsr51801

  Symptoms: Some of the route-maps configured for BGP sessions (eBGP) are not permitting the prefixes upon a router reload.

  Conditions: The symptom is observed when a large number of route-maps for a BGP session are configured and the router is reloaded.

  Workaround: Issue the command **clear ip bgp * soft**.

- CSCsr53059

  Symptoms: A PPPoA session fails to come up after modifying the PVC.

  Conditions: The symptom was seen while testing the feature PPP over ATM with Subscriber Service Switch.

  Workaround: There is no workaround.

- CSCsu58763

Symptoms: Card crashes upon attaching the policy-map to the output interface.

Conditions: This is happening in all types of VCs (PVC/SVC) when the service policy is defined with the **shape** command.

Workaround: There is no workaround.

- CSCsr62645

  Symptoms: Software-forced reload occurs on Cisco 870 router.

  Conditions: Encountered during extended VLAN testing.

  Workaround: There is no workaround.

- CSCsr97753

  Symptoms: Pinging an interface fails.

  Conditions: Occurs when unconfiguring xconnect on the interface.

  Workaround: Perform a **shut/no shut** on the interface.

- CSCsu02975

  Symptoms: Router crashes due to memory corruption.

  Conditions: WAN router crashes when feature combination includes Frame Relay, EIGRP, GRE, QoS, and multicast are configured on WAN aggregation and branches.

  The issue is seen only on PA-MC-2T3/E3-EC and when frame-relay fragment and service-policy is part of map-class frame-relay configurations.

  Workaround: Have either frame-relay fragment or service-policy as part of map-class frame-relay configurations.

- CSCsu50252

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsu65401

  Symptoms: Commands run using the **tclsh** exec command fail with the error:

  ```
  Command authorization failed.
  ```

  Conditions: This occurs in Cisco IOS Release 12.4(20)T if the following is configured on the device:

  ```
  aaa authorization commands 15 default group tacacs+
  ```

  Workaround: The username being passed to the AAA server is an empty string. If there is a default profile on the AAA server that allows all commands to be run, then the **tclsh** exec commands will work. Otherwise there is no workaround.

- CSCsu71818

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

  Conditions: This symptom occurs on a Cisco 7206VXR (NPE-G1) that is very busy running NAT. The router crashes with Cisco IOS Releases 12.4(16a) and 12.4(15)T1.

  Workaround: There is no workaround.

- CSCsv01850

  Symptoms: If “associate application sccp” is configured under “dspfarm profile”, the CLI is split into two lines in **show run**:

```
dspfarm profile 2 transcode universal
  associate application
                                  SCCP
```

This will cause a parser error after a save and reboot.

Conditions: The symptom is observed when “associate application sccp” is configured under “dspfarm profile”.

Workaround: After a reboot, re-enter the command and do a **shut** and **no shut**.

- CSCsv20948

  Symptoms: The primary router may crash continually.

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

  Workaround: There is no workaround.

- CSCsv27607

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

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

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

- CSCsv28451

  Symptoms: A Cisco 7600 PE router fails to redistribute a VRF prefix into BGP after the prefix or path to it flaps. The PE router will indicate the prefix being redistributed into BGP but the prefix will not get installed into the BGP table until the prefix is cleared:

```
PE2#
PE2#sh ip route vrf foo 10.5.5.5

Routing Table: foo
Routing entry for 10.5.5.5/32
  Known via "ospf 1", distance 110, metric 20, type extern 2, forward metric 10
  Redistributing via bgp 666
  Advertised by bgp 666 metric 10 match internal external 1 & 2
  Last update from 10.45.45.2 on Ethernet1/0, 00:00:56 ago
  Routing Descriptor Blocks:
  * 10.45.45.2, from 10.5.5.5, 00:00:56 ago, via Ethernet1/0
      Route metric is 20, traffic share count is 1
PE2#
PE2#sh ip bgp vpnv4 vrf foo 10.5.5.5
% Network not in table
PE2#
```

  Conditions: The PE router redistributing the given prefix must have a sham-link configured for the given VRF and an alternate path to the prefix must exist once the primary (sham-link) is down.

  Workaround: Use the following command: **clear ip route vrf vrfname** *prefix*.

  Further Problem Description: This problem is seen only in Cisco IOS Release 12.2(33)SRB. Cisco IOS Releases 12.2(33)SRC/SRD, etc. are not affected.

- CSCsv29659

  Symptoms: RP configured inside a NAT not shown on test device outside the NAT.

  Conditions: Entering the **show ip pim rp mapping** command fails to display the RP.

  Workaround: There is no workaround.

- CSCsv40340

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

  Conditions: This symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4(15)T7. The router is configured with NHRP.

  Workaround: There is no workaround.

- CSCsv48603

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsv55810

  Symptoms: A Cisco router may reload unexpectedly due to a software forced crash:

  ```
  001286: Nov 5 13:14:22: %SYS-6-STACKLOW: Stack for process AAA Per-User running low,
  0/6000
  %Software-forced reload
  ```

  Conditions: This has been experienced on a Cisco 2811 router running Cisco IOS Release 12.4(20)T1 and 12.4(22)T. The router is configured with AAA.

  Workaround: There is no workaround.

- CSCsv77531

  Symptoms: A device may reload unexpectedly.

  Conditions: The symptom is observed when the device is performing either a CBAC traffic inspection or a Zone-Based Firewall inspection on TFTP.

  Example of vulnerable configuration for CBAC traffic inspection:

  1. TFTP inspection rule is configured: ip inspect name example_name tftp
  2. Apply inspection rule to the interface: interface Ethernet1/1 ip inspect example_name in

  Example of vulnerable configuration for Zone-Based Firewall inspection:

  1. Create a CBAC Class Map: class-map type inspect match-all tftp-traffic match protocol tftp match access-group 100
  2. Create a CBAC Policy Map: policy-map type inspect tftp-inspection class type inspect tftp-traffic inspect

  Workaround: Disable Cisco IOS Firewall inspection for TFTP.

  Further Problem Description: Further information on CBAC is available at:

  http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_content_ac.html

  Further information on Zone-Based Policy Firewalls is available at:

  http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008060f6dd.html

- CSCsv77932

  Symptoms: Router crashes.

  Conditions: Occurs while configuring serial interface for insufficient MTU.

  Workaround: There is no workaround.

- CSCsv79584

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

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

  Workaround: There is no workaround.

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

- CSCsv81176

  Symptoms: Router crashes with syslog CHUNKBADMAGIC.

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

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

- CSCsv85530

  Symptoms: When accounting is enabled for virtual private dial-up network (VPDN), there might be messages with termination cause “nas-error” and displaying impossible values in Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets and Acct-Output-Packets.

  This causes accounting to be unreliable.

  Conditions: This symptom occurs with Cisco IOS Release 12.4T and configured for PPTP/L2TP with accounting.

  Workaround: There is no workaround.

- CSCsv90106

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

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

  Workaround: There is no workaround.

- CSCsv91602

  Symptoms: Cisco 7201 with Gi0/3 experienced communication failure.

  Conditions: This problem does not occur with Gi0/0 or Gi0/2.

  Workaround: Perform a **shut/no shut** on the Gi0/3. The problem will occur again.

- CSCsv96757

  Symptoms: After configuring random detect (WRED) on the ATM interface on a Cisco 888 Integrated Services router and traffic is sent through the VLAN input interface the to ATM interface, the router will display a continuous maclloc error. Additionally, the router crashes within 10-20 seconds after the traffic is stopped.

  Conditions: The problem is only observed on Cisco 888 Integrated Services router when WRED is enabled on the ATM interface.

  Workaround: Do not enable WRED on the ATM interface on the Cisco 888 integrated services router.

- CSCsv97772

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

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

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

- CSCsw18636

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

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

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

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

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

- CSCsw21960

  Symptoms: A router crashes while executing some NAT commands.

  Conditions: The symptom is observed under the following conditions:

  – Try and configure “inside destination translation” with the command before configuring the pool or the access list “ip nat inside destination list ABC pool pool1”.
  – While you configure the above, keep traffic ON.
  – Make sure some active dynamic translations are present while you are configuring this.

  The router does not crash all the time. A combination of the above commands and removing and reconfiguring with traffic can cause the router to crash

  Workaround: There is no workaround.

  Further Problem Description: The crash is not consistently reproducible.

- CSCsw23314

  Symptoms: A router reloads when a manually keyed crypto map is removed from an interface after unconfiguring the tunnel source.

  Conditions: The symptom is observed when the manually keyed crypto map is applied on the tunnel interface. The crash happens when the user cuts and pastes several “no” forms of the CLI in order to delete the tunnel source interface as well as removing the crypto from the tunnel and deleting the tunnel interface itself:

  ```
  conf t
     int tunnel0
     no ip addr x.x.x.x x.x.x.x
     no tunnel source e1/0
     no tunnel dest y.y.y.y
     no crypto map ! must be a manually keyed crypto map
     exit
     no interface tunnel0
  ```

  The issue occurs only on a Cisco 7200 series router with VSA, a Cisco ASR 1000, or a Cisco Catalyst 6000 Series Switch with VPNSPA.

  Workaround: Enter the commands one at a time, waiting after removing the tunnel source. This will prevent the race condition from occurring, avoiding the crash.

- CSCsw24966

  Symptoms: SSL VPN client or AnyConnect client performance drops after a period of operation.

  Conditions: Occurs when Cisco Express Forwarding (CEF) is enabled.

  Workaround: Disable CEF if possible.

- CSCsw29463

  Symptoms: The router, which is configured as a hub in a Dynamic Multipoint VPN (DMVPN), may reload unexpectedly.

  Conditions: The symptom is observed periodically in a scaled configuration when the router is connected to a live network and traffic is passing.

  Workaround: There is no workaround.

- CSCsw36397

  Symptoms: VoIP RTP connections may dangle at TGW when a call failure occurs, due to a performance test.

  Conditions: The symptom is observed during performance testing with many calls (more than 600) run for any duration above 5 minutes. The call failure occurs due to a network timeout issue from SIP server (acting as proxy server) causing hung VoIP connections at the TGW.

  Workaround: There is no workaround.

  Further Problem Description: The problem appears when the SIP server in the network delays responding to the messages sent from OGW and TGW due to network delays. The TGW is unable to clear the VoIP RTP sessions causing the hung RTP connections. If the calls run for more than an hour, the memory gets exhausted in the TGW causing it to crash.

- CSCsw37279

  Symptoms: When using PKI for identifying group members, a group member may fail to register with the key server if the certificate is not installed at the time that Group Domain of Interpretation (GDOI) is enabled.

  Conditions: The symptom is observed when SCEP is used for certificate enrolment.

  Workaround: Clear the current GDOI registration with the following command: **clear crypto gdoi**.

- CSCsw43211

  Symptoms: Following errors are seen:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_to_ptr (bad id) (id: 0xFFFFFFFF)
  -Traceback= 60476EBC 60477400 60491664 616C5834 616C7EEC 61AB72CC 61AC2E64 61AC2EBC
  60FE4274 60FDEFA4 60FD4180 60FD4874 60FD4BBC 60FD275C 60FD27A0 60FC8F74
  ```

  Conditions: This has been seen on a Cisco 7200 after upgrading to Cisco IOS Release 12.2(33)SRC2.

  Workaround: There is no workaround.

- CSCsw50802

  Symptoms: No extra I/O memory is allocated for some HWICs.

  Conditions: This symptom occurs when HWIC is equipped with smart cookie.

  Workaround: Use static I/O memory configuration instead.

- CSCsw52416

  Symptoms: Dynamic NAT entries are not timing out properly

  Conditions: Occurs even after timer expired.

  Workaround: There is no workaround.

- CSCsw52932

  Symptoms: Group members' rekey SAs that have the same IKE SA endpoints (source/destination addresses) are mistakenly deleted when one of the group members has to re-register.

  Conditions: This occurs when one of the group members has to re-register.

  Workaround: Have all the group members re-register at the same time (e.g. reapply the crypto map or use the **clear crypto gdoi** command).

- CSCsw62997

  Symptoms: Traceback is seen while configuring a policy in the virtual-template on LAC.

  Conditions: The symptom is observed when the class-map under the policy has the following filter:

  match vlan *vlan-id*.

  Workaround: There is no workaround.

- CSCsw65933

  Symptoms: The CE does not learn the prefix from one of the PEs.

  Conditions: The symptom is observed after configuring (on PE2):

  ```
  router bgp 10
  address-family ipv4 vrf test1
  no neighbor peer route-map setsoo in
  end
  ```

  and then clearing using the following command: **clear ip bgp** *peer vrf test1* **soft out**.

  Workaround: Use the command **clear ip bgp * soft** on the PE after SOO is applied.

  Alternate Workaround: On the CE, the command **clear ip bgp * soft** should not be applied within one minute after applying SOO route map to CE on UUT.

- CSCsw68022

  Symptoms: A router crashes after unconfiguring SCCP group using the following command: **no sccp ccm group #**.

Conditions: The symptom is observed when SCCP group is configured on the router, and DSPfarm profiles (conference and transcoding) are configured and active on the router. If the commands **no sccp ccm group #** and **dspfarm profile** *id* **conference** followed by **shutdown** are entered at the same time, the router crashes.

Workaround: Do not enter the commands **no sccp ccm group #** and **dspfarm profile** *id* **conference** followed by **shutdown** at the same time.

- CSCsw69069

  Symptoms: During the session, assigned IP address of the client changes, and after the session is finished only the last IP address is released. This causes IP pool exhaustion, which can be solved only by a reload.

  Conditions: Occurs on AnyConnect client on Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsw70204

  Symptoms: WISPr attributes could cause memory leak in ProxyLogon situation.

  Conditions: The symptom is observed when the subscriber logs on using WISPr attributes.

  Workaround: There is no workaround.

- CSCsw77293

  Symptoms: Upon unconfiguring “channel-group” in one controller, the ping fails in another controller.

  Conditions: The symptom is observed when a controller is configured and then unconfigured with “channel-group”.

  Workaround: Configure “channel-group” again.

- CSCsw78413

  Symptoms: The BFD configuration may be lost from the interface/sub-interface upon a router reload or physical module of OIR.

  Conditions: The symptom is seen when BFD is configured on an interface in certain multi-slot chassis.

  Workaround: Ethernet interfaces seem immune to this problem. Certain platforms, such as the Cisco 10000 series router, are also immune.

- CSCsw78879

  Symptoms: The secondary key server crashes when it sends a KEK rekey to the GMs soon after it takes over as the primary key server.

  Conditions: The symptom is seen when the secondary key server switches to primary just before it is time to send the KEK rekeys to the group members. This problem can be seen in any co-operative key server environment.

  Workaround: There is no workaround.

- CSCsw80640

  Symptoms: A Cisco router may experience the following errors:

```
%SYS-2-SHARED: Attempt to return buffer with sharecount 0, ptr= 659594E0
-Process= "IP Input", ipl= 4, pid= 93,
-Traceback= 0x60C6C978 0x60373164 0x61556FC8 0x61558534 0x612D6A44 0x612D8368
0x612D8780 0x612D883C 0x612D8A84
%SYS-2-SHARED: Attempt to return buffer with sharecount 0, ptr= 6649466C
```

```
-Process= "IP Input", ipl= 4, pid= 93,
-Traceback= 0x60C6C978 0x60373164 0x61556FC8 0x61558534 0x612D6A44 0x612D8368
0x612D8780 0x612D883C 0x612D8A84
```

Conditions: This symptom is observed on a Cisco 2801 router that is running Cisco IOS Release 12.4(20)T. The errors appear to be triggered with the forwarding of UDP packets.

Workaround: There is no workaround. The problem does not appear to be service impacting.

- CSCsw84994

  Symptoms: A Cisco 7301 router may experience a lot of CPU hogs due to the SSGTimeout process:

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

  Conditions: The symptom is observed on a Cisco 7301 router that is running Cisco IOS Release 12.4(21).

  Workaround: There is no workaround.

- CSCsw85293

  Symptoms: The following CPUHOG messages are seen for Crypto ACL process:

  ```
  %SYS-3-CPUHOG: Task is running for (xxxx)msecs, more than (2000)msecs (9/7),process =
  Crypto ACL.
  ```

  Conditions: This has been seen on Cisco routers that are running Cisco IOS Release 12.4(15)T8 (other versions may be affected as well) with GETVPN configured.

  Workaround: Reducing the size and complexity of the crypto ACLs will often stop these errors.

- CSCsw90055

  Symptoms: An FXO port with “supervisory disconnect tone” configured is unable to be released while receiving disconnect tone.

  Conditions: The symptom is observed when FXO is handling a fax call which will disable the FXO port “supervisory disconnect tone” capability and cause the FXO to be unable to detect the disconnect tone.

  Workaround: There is no workaround.

- CSCsw97262

  Symptoms: The command **analysis-module** is not replicating packets routed from an IP Phone.

  Conditions: The symptom is observed on an IP Phone communication set up via router to FXO. Ingress interface contains the **analysis-module monitoring** command.

  Workaround: There is no workaround.

- CSCsw98414

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

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

  Workaround: There is no workaround.

- CSCsw99846

  Symptoms: With mLDP over a P2P tunnel, traffic drops in multiple cases.

  Conditions: The traffic drops when there is a change in path set entries, which can happen when you perform a **shut** and **no shut** the TE tunnel or toggle MPLS traffic-tunnel or use the **clear mpls traffic-eng auto-tunne** command.

  Workaround: There is no workaround.

- CSCsx07423

  Symptoms: The router stays at 100% CPU usage after trying to establish an SSL session with an SSL server when this SSL server is not reachable.

  Conditions: The symptom is observed with any applications on the router that use an SSL client to establish a secure session with the SSL server. At the same time, the secure server is not available for whatever reason.

  Workaround: Make sure the SSL server is reachable by pinging it. Save the configuration as startup-config and reload the router.

- CSCsx08292

  Symptoms: When Service Policy is applied under the PVC, traffic flow across that interface stops.

  Conditions: The ping failure starts only after service-policy configuration.

  Workaround: There is no workaround.

- CSCsx09343

  Symptoms: PKI daemon is stuck in DNS resolution attempt for the hostname used in the CDP.

  Conditions: The symptom is observed when using name resolution for automatic actions taken by the router during non-interactive sessions (CRL download using name in CDP URI). This issue has been seen to occur only on a Cisco Catalyst 6500 running Cisco IOS SXH software.

  Workaround: There is no workaround.

- CSCsx15358

  Symptoms: A router may crash after receiving DNS TCP queries.

  Conditions: The symptom is observed on a router with “ip dns server” configured.

  Workaround: There is no workaround.

- CSCsx19184

  Symptoms: Router crash due to Address Error:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0xXXXXXXXX
  ```

  Conditions: This has been seen on Cisco routers running 12.4T and 12.4 images with SIP traffic.

  Workaround: There is no workaround.

- CSCsx20984

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

  Conditions: Unknown at this time.

  Workaround: There is no workaround.

- CSCsx23602

  Symptoms: A Cisco Catalyst 6000 that is running modular Cisco IOS 12.2(33)SXH4 may crash with NAT configuration.

  Conditions: This symptom occurs when running modular Cisco IOS with NAT deployment. Crash is only happening in production, and NAT translation is required for crash to occur.

  Workaround: Run non-modular Cisco IOS Release 12.2(33)SXH4.

- CSCsx25880

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free

software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml.

- CSCsx29278

  Symptoms: Traceback will be seen if high amount of HTTP sessions are sent with Java blocking enabled.

  Conditions: Occurs on Cisco 3845 and Cisco 7200G1 routers with high number of HTTP connection per second and with HTTP inspection with Java blocking enabled. May occur on other platforms.

  Workaround: Does not impact router functionality. The issue can be avoided by not enabling Java blocking.

- CSCsx29605

  Symptoms: QSIG-rose memory leak is seen with QSIG MWI feature enabled. The topology is:

  Avaya phones----Avaya PBX---QSIG----ISR----SIP-----IP Unity Voice Mail

  Conditions: The leak is observed per call during the following call scenario, Leave Message -> MWI ON -> Retrieve Message -> MWI OFF.

  Workaround: There is no workaround.

- CSCsx29726

  Symptoms: If fail-close is unconfigured when a GDOI crypto map is in fail-close mode (after an unsuccessful registration), the crypto map will drop all unencrypted traffic regardless of a subsequent successful registration.

  Conditions: The symptom is observed when a GDOI crypto map configured with fail-close. Fail-close is unconfigured while crypto map is in fail-close mode.

  Workaround: Remove and reapply the crypto map to the interface or the fail-close configuration.

- CSCsx33622

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

  Conditions: This issue is seen only in topologies where a Cisco IOS device is communicating with a non-Cisco-IOS peer or with a Cisco IOS device on which this defect has been fixed. The router with the fixed Cisco IOS software must advertise a lower maximum segment size (MSS) than the non-fixed Cisco IOS device. ICMP unreachables toward the non-fixed Cisco IOS router must be turned off, and TCP options (for example, MD5 authentication) and the **ip tcp path-mtu-discovery** command must be turned on.

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

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

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

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

- CSCsx34297

  Symptoms: Watchdog reset seen with combination of NPEG1+PA-POS-1OC3/PA-POS-2OC3.

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

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

- CSCsx34703

  Symptoms: In certain corner cases, received BFD packets can fill up the input queue on the incoming interface eventually blocking packet reception on that interface.

  Conditions: The symptom is observed when BFD is enabled and BFD adjacency is established after bootup.

  Workaround: There is no workaround.

- CSCsx35306

  Symptoms: Router crashes at “t3e3_ec_safe_start_push”.

  Conditions: The crash is seen immediately after removing the channel-group of the PA-MC-2T3/E3-EC card.

  Workaround: There is no workaround.

- CSCsx41624

  Symptoms: In a rare situation 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.

  Conditions: The symptom is observed when the SSLVPN process is waiting for HTTP REQUEST from a client on the port configured using **http-redirect <port no>** and never wakes up. This can happen because of an unexpected IPC message to SSLVPN process by another IOS process.

  Workaround: Remove **http-redirect**.

- CSCsx45429

  Symptoms: The GM crashes when trying to display VSA policy detail using the **show pas vsa policy detail** command and when traffic is being sent through the GM.

  Conditions: The symptom is observed when using the **show pas vsa policy detail** command. It may affect all recent software releases.

  Workaround: There is no workaround.

- CSCsx45923

  Symptoms: On a router that has a Virtual Tunnel Interface (VTI) IPSEC configuration, an access control list (ACL) may be bypassed when there is an ACL on the tunnel interface. This happens only in the case where the physical interface (facing the ipsec peer) also has a ACL.

  Conditions: This symptom is observed when there is a ACL configured on the physical interface (facing the ipsec peer)

  Workaround: Apply the ACL on the protected LAN interface in the outbound direction, instead of on the tunnel interface

- CSCsx46421

  Symptoms: The file transfer aborts with the Active FTP.

  Conditions: The symptom is observed with the image c7200-adventerprisek9-mz.124-23.15.T3.

  Workaround: Use Passive FTP (**ip ftp passive**) for the FTP file to be properly transferred.

- CSCsx47227

  Symptoms: Incoming traffic on a PBR-configured interface is process switched.

  Conditions: The symptom is observed when traffic ingressing on an interface configured for PBR when using an ipbase, ipvoice, or entbase Cisco IOS images.

  Workaround: Disable PBR on the incoming interface.

- CSCsx51103

  Symptoms: Router crashes at an OCE function in crypto switching code.

  Conditions: The symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4(20)T, 12.4(22)T and 12.4(24)T. The following steps are used to generate the crash:

  1. Start VPN client and initiate connection.
  2. After successful connection, open DOS prompt.
  3. Start a trace route (tracert) to an internal IP OR start to an external IP.

  Workaround: There is no workaround.

- CSCsx51355

  Symptoms: Cisco 3845 used as a WAN aggregator will randomly crash when Frame Relay fragmentation is configured and with high traffic.

  Conditions: This symptom occurs when branch routers are configured with FR, EIGRP, GRE, QOS, and Multicast. Traffic is sent. This symptom occurs in an internal build of Cisco IOS Release 12.4(24)T.

  This crash only happens when:

  1. Frame-relay is configured together with the QoS policy, and packet size is larger than the fragment size.
  2. Traffic exceeds 50% of line rate.

  Workaround: Remove the FR fragmentation configuration.

- CSCsx51792

  Symptoms: The basic ping fails between two end-to-end ATM interfaces.

  Conditions: The symptoms are observed when two end-to-end ATM interfaces are configured. The ping fails.

  Workaround: There is no workaround.

- CSCsx55741

  Symptoms: Transit IPsec traffic is dropped on GM GETVPN. The following message is shown:

  ```
  %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
  destaddr=192.168.6.1, prot=50, spi=0xC39A071A(3281651482), srcaddr=192.168.6.2
  ```

  Conditions: The symptoms are observed under the following conditions:

  1. A Cisco 7200 series router in combination with VSA as HW-accelerator.
  2. GDOI policy defined to not perform double encryption.
  3. R1 connects to R2[GM], connects to R3[GM], connects to R4. (R2 and R3 are two group members of a GETVPN networks.) The GDOI policy is: Deny R1=>R4; Deny R4=>R1; Permit any any.

Workaround: Permit double encryption with the following caveat: If transiting ESP packet are near the IPsec path MTU then, after encapsulation into GETVPN IPSEC, they will be fragmented. The receiving side of the transit IPsec flow (e.g. R1 or R4 in above scenario) will have to reassemble these packets which can lead to high CPU on the receiving end.

This makes the workaround more or less applicable depending on the transiting traffic partern.

- CSCsx58009

  Symptoms: SAMI PPC crashes due to a SegV exception at the L2TP process.

  Conditions: The symptom is observed under the following conditions:

  1. L2TP communication down keeps more than 180 seconds between LAC and LNS.
  2. Crash will occur where the communication down happens after about 17 seconds from receiving the last L2TP hello.

  Workaround: Avoid sending L2TP hello at L2TP shutting down process by L2TP shutdown timer expiration. (For example, use **l2tp tunnel timeout no-session 0**. The command will tear down the session immediately when there is no session.)

- CSCsx60891

  Symptoms: A numbered ACL with an object-group reference is not nvgened properly.

  Conditions: Global (numbered) ACL configuration mode does not support OG. (You can configure OG for numbered ACLs using sub-configuration (named) mode.) This issue applies only to numbered ACLs.

  Workaround: Use named ACLs in place of numbered ACLs.

- CSCsx63982

  Symptoms: A router configured for SNMP might unexpectedly crash with a bus error code.

  Conditions: This issue occurs when you query cSipCfgPeerTable of CISCO-SIP-UA-MIB. To be more specific, cSipCfgPeerPrivacy MIB object.

  Workaround: Do not poll cSipCfgPeerPrivacy MIB object.

- CSCsx67084

  Symptoms: Police policy is not working at Multilink interface with MPLS EXP classification.

  Conditions: This symptom is seen with a Cisco 7200 series router after detach a 3 level policy. In a 3 level policy, police is configured at level 3. After detach 3 level policy, attach a single level policy with police class.

  Workaround: There is no workaround.

- CSCsx68254

  Symptoms: Device will crash when loading the configuration with service policies with ACLs.

  Conditions: This is seen when more than 200 ACL filters are used in a service policy.

  Workaround: Remove unused ACLs in class-maps to get under the 200 limit. (The fix allows for 512 filters.)

- CSCsx70889

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsx74151

  Symptoms: Large packets may be dropped if prefragmentation is enabled with VSA.

  Conditions: The symptom is observed when GETVPN creates some tunnels with time-based anti-replay and others with counter-based anti-replay/no anti-replay.

  Workaround: Use the same replay method for all the SAs in the router.

- CSCsx75004

  Symptoms: In a Carriers Carrier, the CSC-PE router advertises wrong out-label. This causes the end-to-end LSP to be broken in the CSC network, and all traffic is dropped.

  This problem is observed by enabling the **show ip bgp label** command on CSC-CE. See "Out Label" of the route is "imp-null".

  Conditions: This condition is observed in routers that are running Cisco IOS Release 12.0(32)SY6.

  Workaround: Configure **neighbor** {*ip-address* | *peer- group-name*} **next-hop-self** on CSC-PE.

- CSCsx82690

  Symptoms: A voice gateway placing ISDN calls will exhibit a memory leak. The effects of this memory leak can be seen with the **show process memory** command. It shows that the amount of memory the ISDN process is holding continues to increase without being released.

  Conditions: The symptom is observed on a voice gateway that is processing ISDN calls on a PRI interface. Switchtype is set to be primary-QSIG and the calls that leak memory are QSIG-GF (connection-oriented calls) and not regular voice calls. Such calls are typically used when implementing supplementary services such as MWI.

  Workaround: There is no workaround.

- CSCsx94324

  Symptoms: Packets with certain packet sizes get dropped when being CEF-switched on a router.

  Conditions: The symptom is observed when CEF is enabled and when the outbound interface is an HWIC-4SHDSL DSL interface. It is observed when the packet undergoes fragmentation.

  Workaround: Disabling CEF is a workaround.

- CSCsx96381

  Symptoms: A video conference device makes a video call to a TDM Conference Station through an H320 gateway. When the call is placed, only the primary channel goes up and the H320 gateway does not proceed with secondary channels.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsx98284

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

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

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

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

  Alternate workaround: Separate the MTP functionality from the gateway.

- CSCsy05298

  Symptoms: The IOSD-crash is seen and is affecting the main functionality.

  Conditions: This symptom is observed when a large number of groups (i.e. 50) is configured. The IOSD-crash is seen when we give the **show crypto gdoi** command after applying the general configuration and after checking the ping between all the PIM neighbors.

  Workaround: Use the **show crypto gdoi group** *group- name* to display a specific group's information.

- CSCsy07369

  Symptoms: An invalid range of IP addresses are accepted at CLI.

  Conditions: The symptom is observed when the following command format is used: **range** *ipaddress1 ipaddress2* where the range of the IP addresses is not seen in same network.

  Workaround: Avoid entering wrong ipaddress2.

- CSCsy09101

  Symptoms: Cisco Configuration Professional (CCP) is unable to load signatures from the router. Cisco IOS-IPS signatures cannot be viewed or modified using CCP.

  Conditions: The symptom occurs when using CCP to manage IPS5.0 in routers that are running Cisco IOS Release 12.4(20)T2, 12.4(24)T and 12.4(22)T1.

  Workaround: There is no workaround from CCP. Use CLI to view or modify IPS signatures.

- CSCsy10653

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

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

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

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

     mgcp behavior g729-variants static-pt

     mgcp behavior dynamically-change-codec-pt disable

  2. Disable g729br8 from being negotiated for this call. If CUCM is involved, this is done with the service parameter "Strip G.729 Annex B (Silence Suppression) from Capabilities".
  3. Use a Cisco IOS code on the gateway which does not contain the fix for CSCsu66759 (Cisco IOS Release 12.4(22)T and below).

- CSCsy15227

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

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:

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

- CSCsy15468

  Symptoms: Crash keyserver reloads.

Conditions: The symptom is observed if test case 1 in TBAR sanity regression on the VSA is configured and then unconfigured. When configuring the second one, the keyserver crashes.

Workaround: There is no workaround.

- CSCsy16092

  Symptoms: A Cisco router that is running Cisco IOS or Cisco IOS XE may unexpectedly reload due to watchdog timeout when there is a negotiation problem between crypto peers.

  The following error will appear repeatedly in the log leading up to the crash:

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

  Conditions: The device must have “debug crypto isakmp” enabled.

  Workaround: Turn off the debug.

- CSCsy16220

  Symptoms: A switch may reload with messages on both the RP and SP similar to:

  ```
  %CPU_MONITOR-2-NOT_RUNNING: CPU_MONITOR messages have not been sent for 30 seconds
  ```

  Conditions: The symptom is observed with SNMP polling configured for SNMP MIB:

  ```
  ceemEventMapEntry, oid 1.3.6.1.4.1.9.10.91.1.1.1.1
  ```

  This crash will only occur on modular IOS.

  Workaround: Disable SNMP polling of SNMP MIB:

  ```
  ceemEventMapEntry, oid 1.3.6.1.4.1.9.10.91.1.1.1.1
  ```

- CSCsy19659

  Symptoms: When using Point-to-Point Tunnelling Protocol (PPTP) with RADIUS Accounting, there may be several “nas-error” and “lost-carrier” listed in accounting as the Acct-Terminate-Cause.

  Conditions: The symptom is observed when using Cisco IOS Release 12.4T (Releases 12.4(15)T-12.4(22)T confirmed) and using PPTP with RADIUS Accounting in place.

  Workaround: There is no workaround.

- CSCsy20488

  Symptoms: IPSsec/GRE traffic does not go over an ATM interface.

  Conditions: The symptoms are observed when using a VSA encryption card and when the ATM interface is using PVC bundles.

  Workaround: Do not use PVC bundles.

  Alternate workaround: Disable the VSA encryption and use software encryption (not recommended for a high load of encryption).

- CSCsy22826

  Symptoms: The VG224 endpoint does not connect to the callback destination, once the callback destination is idle.

  Conditions: The symptom is observed with a multi-node cluster and when a VG224 endpoint is registered with a node other than the first node in the cluster.

  Workaround: Have VG224 endpoints registered with the first node.

  Further Problem Description: The activation of the callback is successful. The failure is when the callback destination becomes idle again and the VG224 endpoint gets notified (ring). After the VG224 endpoint goes offhook, the system should automatically connect to the callback destination. This does not happen and VG224 endpoint gets silence.

- CSCsy22920

  Symptoms: A router crashes at mripv6_mode_entry when the authentication key is configured to be equal to 64 bytes.

  Conditions: The symptom is observed on a router that is running the c7200-adventerprisek9-mz.124-24.6.T image.

  Workaround: Configure an authentication key of less than 64 bytes.

- CSCsy24676

  Symptoms: On occasion, a false positive is returned on a file system failure. File operation is deemed successful when, in fact, it has failed.

  Conditions: This problem occurs when the file system device returns an error and the code follows the path in the file system buffer cache where the error is masked and converted to a success code. This problem is likely to show up if there is a device error during the write. The device error may be due to bad media or an OIR (although it is very unlikely during an OIR).

  Workaround: There is no workaround.

  Further Problem Description: This is possible during any file system operation where a file system device is unable to complete the operation and an error is returned. This error is not passed down to the file system stack but is converted to a success code. Other clients which are dependent on previous file system operations fail on successive file system calls and possibly result in a crash.

- CSCsy27394

  Symptoms: Users who can execute a **show ip interface** command can see that an LI tap is in progress.

  Conditions: No specific conditions are necessary to trigger this problem.

  Workaround: There is no workaround.

- CSCsy28758

  Symptoms: HLog softkey stops working.

  Conditions: The symptom is observed under the following conditions:

  1. When logging into an EM profile where the user was logged out from the hunt group.
  2. This is to be done on a phone where an EM profile was previously logged in, which was also logged into the huntgroup.

  Workaround: Log in with the EM profile on the phone that was used to log out the huntgroup.

- CSCsy29828

  Symptoms: A Cisco router may reload due to a bus error. The error indicates trying to read address 0x0b0d0b**, where ** is around 29.

  Conditions: This has been experienced on a Cisco 2800 series router running Cisco IOS Release 12.4(24)T. The router must be configured with NAT, and SIP traffic is passed through the NAT router.

  Workaround: Enter the following commands:

  * **no ip nat service sip tcp port 5060**

  * **no ip nat service sip udp port 5060**

  Or

  * **ip nat translation timeout never**

- CSCsy31365

  Symptoms: Memory leak of 24-bytes can occur when a transcoding call is disconnected.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(24.6)T and is seen while shutting down the DSPfarm profile when the transcoding call is active in IPIPGW.

  Workaround: There is no workaround.

- CSCsy32146

  Symptoms: Through-the-box traffic is dropped on the router (when the egress path is from the clear-text side to the encrypted side).

  Conditions: The symptom is observed with Cisco IOS Release 12.4(20)T and with L2TP over IPSec with a front door VRF.

  Workaround: Disable **ip route-cache** and **ip route-cache cef** on the clear-text interface (where the clear-text traffic comes from).

- CSCsy33068

  Symptoms: A big SDP HTML template causes an abrupt termination of the SDP process.

  Conditions: The HTTP post to the HTTP server in an IOS router is size-limited. The limit is set to 32KiB by default. In the SDP process, the transition from introduction page to the completion page involves an HTTP post. The post contains information including the SDP bootstrap configuration and the completion template together with the overhead of HTTP post communication. The size limit might be reached with moderate usage of HTML elements. The HTTP post in SDP is base-64 encoded. The total size limit of the SDP bootstrap and the completion template is roughly (32KiB - 2KiB(overhead)) * 3/4(base-64 encoding) = 22.5KB.

  Workaround: Reduce the size of the HTML template, and abridge the configuration. The total size of the two cannot exceed ~22.5KB. Example of abridged configuration:

```
configure terminal => config t
 Interface FastEthernet 1 => int Fa 1
```

- CSCsy45371

  Symptoms: The **clear ip nat tr *** command removes corresponding static NAT entries from the running configuration, but removing static NAT running configuration does not remove the corresponding NAT cache.

  Conditions: Occurs when NAT commands are entered while router is processing around 1 Mb/s NAT traffic.

  Workaround: Stop the network traffic while configuring NAT.

- CSCsy54068

  Symptom: HQF policer policy with exceed action does not attach. Or, when execute exceed action is in an attached parent policy, policy is removed from the interface.

  Conditions: This symptom is seen in a two level, two rate, two color policy.

  Workaround: There is no workaround.

- CSCsy54122

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsy55800

  Symptoms: OSPF route gets stuck in the RIB.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(15)T and later. It is seen if a valid LSA for the same network exists but is filtered via a route-map.

  Workaround: Using the command **clear ip route X.X.X.X** will temporarily fix the issue, but the problem will reoccur each time the permitted route is withdrawn.

- CSCsy58115

  Symptoms: In a router running BGP, the BGP process may hold increased amounts of memory over time without freeing any memory. This may also be seen from the output of **show proc mem sort** and in the output of **show ip bgp sum** or **show ip bgp vpnv4 all sum** and looking at the number of BGP attributes which may be increasing over time in relation to the BGP prefixes and paths which may remain roughly the same.

  Conditions: Some BGP neighbors are not in established state and exchanging prefixes. The issue is observed on all platforms running the following releases of Cisco IOS:

  - 12.2(31)SB14
  - 12.2(33)SB1b
  - 12.2(33)SB2
  - 12.2(33.05.14)SRB
  - 12.2(33.02.09)SRC
  - 12.2(33)SRC3
  - 12.4(20)T2
  - 12.4(22)T1
  - 12.2(33)SXI or later releases.

  Workaround: Remove the configuration lines related to the inactive neighbors (neighbors in Idle or Active states).

- CSCsy58984

  Symptoms: A device that is running Cisco IOS Release 12.4(24)T reloads when editing ACL with an object group.

  Conditions: The symptom is observed on a Cisco 3845 and 2800 series router that is running Cisco IOS Release 12.4(24)T and 12.4(24.6)T2.

  Workaround: Avoid using “range” in any of the object groups (either direct or nested) and containing a group of objects which use a range of IP addresses.

- CSCsy61209

  Symptoms: An IP-to-IP gateway (IPIPGW), also called CUBE, is adding an incorrect token in the H225 connect message.

  Conditions: The symptom is observed on an IPIPGW running Cisco IOS Release 12.4(20)T1, with talking H323 signaling protocol on both sides with security enabled.

  Workaround: There is no workaround.

- CSCsy70619

  Symptoms: A router may crash when multipath is enabled and when the MR is registered with two or more of its roaming interfaces.

Conditions: The symptom is observed when using the **no ip mobile router-service roam** command on any one of the MR's roaming interfaces.

Workaround: There is no workaround.

- CSCsy71006

  Symptoms: When the configured TEK lifetime is greater than 65000, the remaining TEK lifetime on the secondary KS shows zero.

  Conditions: The symptom is observed with a GDOI keyserver and where the TEK lifetime is configured to be greater than 65000.

  Workaround: Use a TEK lifetime of less than 65000.

- CSCsy71258

  Symptoms: Unable to boot a Cisco 850 series router using Cisco IOS Release 12.4(15)T9.

  Conditions: The symptom is observed on a Cisco 850 series router with 64MB of dram. The image requires more dram to boot.

  Workaround: There is no workaround.

- CSCsy73838

  Symptoms: Connection for TR-069 is lost to the device after the device reloads.

  Conditions: The symptom is observed under the following conditions:

  1. Enable CWMP in the router. Inform is sent to ACS. 2. Router is reloaded with CWMP-enabled in the startup configuration. 3. When the router is reloaded, it sends the Inform request to ACS. In this Inform request, a ConnectionRequestURL value is formed without the ProductClass value. 4. ACS can not initiate a connection to the router with the ConnectionRequestURL sent in the Inform request.

  Workaround: There is no workaround.

- CSCsy74329

  Symptoms: The following message appears on the console:

  ```
  [crypto_bitvect_alloc]: bitvect full (size = 8192)
  -Traceback= 0x4244AB0 0x426875C 0x426AE60 0x426B330 0x426FAF4 0x4292B7C 0x4293278
  0x75429C
  ```

  Conditions: The symptom is observed when the GetVPN rekey is used with a number of Deny ACL entries and with VSA.

  Workaround: There is no workaround.

- CSCsy76185

  Symptoms: The following traceback may be seen:

  ```
  Local7.Critical 192.168.133.252 827681: %SYS-2-NOBLOCK: printf with blocking disabled.
  Local7.Critical 192.168.133.252 827682:
  -Process= "IP Input", ipl= 0, pid= 61 Local7.Critical 192.168.133.252 827683:
  -Traceback= 0x11EF3E4 0x1203120 0x180214C 0x1209F54 0x120A0B8 0x179EF5C 0x19A1F94
  0x19A270C 0x19A2930 0x19A2B0C 0x196B6FC 0x196EC44 0x197115C 0x1972F8C 0x17AC2F4
  0x17AC87C
  ```

  Conditions: The symptom is observed during basic function.

  Workaround: There is no workaround.

- CSCsy77191

  Symptoms: Native GigE interfaces of a Cisco 7200 NPE-G2 router will not acknowledge reception of pause frames and will not stop its transmission in case of media-type RJ45.

Conditions: The symptom is observed with media-type RJ45 and with SFP with “no neg auto” configured.

Workaround: There is no workaround.

Further Problem Description: There are no issues with SFP with a “neg auto” configuration.

- CSCsy79176

  Symptoms: Need to disable CEF to pass IP traffic. With CEF enabled, traffic fails to pass.

  Conditions: The symptom is observed on a Cisco 2801 and 2811 router that is running the ipvoicek9-mz.124-23_15_PI10 image.

  Workaround: Disable CEF OR shut/unshut the interface with incomplete adjacency (using the **show adjacency** command).

- CSCsy79301

  Symptoms: A router crashes when a multicast group address joins and leaves the MLD group from the client within the configured delay time.

  Conditions: The symptom is observed when applying MLD leave for the group for which accounting has not yet started.

  Workaround: There is no workaround.

- CSCsy81339

  Symptoms: The device crashes due to a bus error (CPU signal 10).

  Conditions: This symptom is observed on a Cisco 3825 router that is running c3825-advipservicesk9-mz.124-20.T1.bin. The crash occurs while removing some classes (no class <x>) from a policy-map that is applied on an interface.

  Workaround: There is no workaround.

- CSCsy84229

  Symptoms: When an HTTP request with payload of greater than 10MB is sent to the HTTP server of the router, the server is not able to process the request and responds back with the message “request entity too large”.

  Conditions: The symptom is observed with Cisco IOS Releases 12.4(22)T and 12.4(24)T and when the payload is above 10MB

  Workaround: Updating the signatures from S385 is a potential workaround.

  Further Problem Description: This behavior is only evident while applying S386 and above on devices that do not have any previous signature package. This error does not appear while updating signature from S385 to S386.

- CSCsy84286

  Symptoms: Router crashes while removing “ip dhcp class”.

  Conditions: The symptom occurs with relay agent information and relay-information hex configured.

  Workaround: There is no workaround.

- CSCsy87674

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

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

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

- CSCsy90542

  Symptoms: Multicast traffic is dropped at decrypting side.

  Conditions: This symptom occurs when traffic ACL on the KS is of the type:

  ```
  permit ip host address any
  permit ip any host address
  ```

  Workaround: There is no workaround.

- CSCsy91748

  Symptoms: An NM-CEM-4SER module crashes.

  Conditions: The symptom is observed with an NM-CEM-4SER module when its payload size is changed on a CEM port which is part of a multiplexed group that is created using the **attach** *port* command.

  Workaround: Reload the router after using the **write config** command.

- CSCsy93054

  Symptoms: WebVPN portal is not displayed. The router closes the SSL negotiation as soon as it sends an SSL “Server Hello” message by sending a TCP FIN.

  Conditions: The symptom is observed when a trustpoint uses a certificate chain of larger than 4096 bytes.

  Workaround:

  1. Use a smaller certificate chain.
  2. Use self-signed certificates.

- CSCsy95484

  Symptoms: Ping fails from gen to ref.

  Conditions: The symptom is observed when the router is loaded with Cisco IOS Release 12.4(24.6)T5.

  Workaround: Perform a **shut** and **no shut** on the VLAN interface and the ping passes.

- CSCsy97506

  Symptoms:

  Case 1: All NAT multicast data packets are processed by software.

  Case 2. Spurious memory access occurs.

  Conditions:

  Case 1. NAT with static port entry, or dynamic overload configuration.

  Case 2. Configure **ip nat dynamic nat** rule with an undefined NAT pool.

  Workaround:

  Case 1: Configure NAT as static entry without port, or dynamic non-overload.

  Case 2: Configure with defined pool.

- CSCsy97820

  Symptoms: False positives are seen in matching object groups with variable masks.

  Conditions: The symptom is observed when non-matching traffic is sent.

Workaround: Do not use variable masks and contiguous masks, such as 255.0.255.255. Use only contiguous masks.

- CSCsz16386

  Symptoms: Router will reboot and also causes traceback output.

  Conditions: This happens when running check syntax mode. In syntax mode, when a user enters the event manager applet submode and execute the **no event manager applet** *xxx* two times, this will cause the reboot. “xxx” is the applet name specified when the user enters the submode.

  Workaround: Do not run the **no event manager applet** *xxx* command in check syntax mode.

- CSCsz16635

  Symptoms: One-way audio may be experienced on a call which traverses a transcoder hosted on an ISR platform (e.g.: Cisco 2800, 3800 etc.) after a hold, resume, or transfer.

  Conditions: When the call is held or resumed, there is a significant change in the RTP Sequence Numbers but the SSRC does not change. This behavior may cause the receiving device to assume that the RTP packets are out of sequence (i.e.: late, early, or lost) and therefore the receiving device may drop them.

  Workaround:

  1. A hold/resume from the phone receiving the out-of-sequence RTP audio packets will restore normal reception of audio.
  2. If possible, use a Communications Media Module (CMM) module for transcoding while ensuring that the Cisco IOS Release used on the CMM module has the fix for CSCsi27767.
  3. If possible, eliminate the need for a transcoder in the audio path for affected call flows.
  4. This problem does not affect Cisco IOS Software Media Termination Points (MTPs) nor SW MTPs hosted on a Cisco Unified Communications Manager (CUCM) server. So, if like-to-like capabilities (i.e.: codec and packetization) are being used, then using a SW MTP via IOS or CUCM may be an option.

  Further Problem Description: This issue looks very similar to CSCsi27767 which was opened and resolved against the Catalyst 6000’s CMM. The fix for CSCsi27767 is, however, only intended for the CMM platform.

  Cisco IOS DSPFarm services and voice gateways will now avoid generating discontiguous RTP sequence numbers with the same SSRC, by using a new SSRC and setting the marker bit of the first RTP packet for the new SSRC whenever its DSP restarts the RTP sequence number due to call features such as call transfer, hold, resume, etc.

- CSCsz16941

  Symptoms: A TR-069 Agent becomes disabled on the router and the device is unreachable from the ACS server.

  Conditions: The symptom is observed when a TR-069 Agent is enabled and running on a router and the default WAN interface is configured and has a DHCP-assigned IP address. When the configurations are saved and the router is reloaded the issue is seen.

  Workaround: If possible, do not save the configurations on the router when the WAN interface gets a DHCP-assigned IP address.

  Alternate workaround: Use the **write erase** command and remove all the configurations just before every router reload.

- CSCsz23951

  Symptoms: NSAP address family cannot be configured.

Conditions: The symptom is observed with the initial configuration.

Workaround: There is no workaround.

- CSCsz29815

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

  Conditions: The issue has been reported on the router that is running Cisco IOS 12.4(24)T and configured with TTY lines accessed via reverse SSH Version 2. Issue also affects SSH version 1 where VTY lines get affected.

  Workaround: Reload the router.

- CSCsz38104

  The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload. Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml.

- CSCsz48392

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

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

  Workaround: There is no workaround.

- CSCsz52576

  Symptoms: The vlan.dat file gets deleted after the second reload of the router, and the VLAN definition and names are lost (not the interfaces and IP addresses). It has been observed that when the vlan.dat is lost, in “sh vtp status” the VTP Domain Name is blank (and was properly configured before).

  Conditions: This behavior is observed in a Cisco 3270 router that is running Cisco IOS Release 12.4(24)T. It is also observed with Cisco 1800 ISR with switch modules in Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround. Customer needs to reconfigure them again after reboot. This problem is not observed in Cisco IOS Release 12.4(15)T.

  Further Problem Information: When a customer is running an image that does not store the VTP and VLAN information in the start-up configuration or the normal output of show running-config, the vlan.dat file gets overridden to the default vlan.dat approximately 2 minutes after reboot. The current VLANs and VTP information remains operational until the router is rebooted.

  A reboot causes the VLANs and VTP information to disappear because the start-up configuration does not contain any VLAN or VTP information, nor does the vlan.dat file in flash.

  The operating VTP information appears in the output of show running-config all (which shows non-default and default values), indicating that the router considers the VTP information to be at default values even when there is a VTP domain name configured. This allows the VLANs and VTP to remain operational until the router is rebooted.

- CSCsz53177

  Symptoms: When running Network Load-balancing (IGMP-mode) in VLANs with PIM enabled and static ARP entries for unicast IP to layer-2 multicast address, packet duplication will occur.

Conditions: This symptom occurs when sending unicast (non-multicast) IP packets with multicast layer-2 destinations.

Workaround: Use non-IGMP NLB modes (unicast or multicast with static macs) or use IGMP snooping querier instead of PIM on NLB SVIs.

- CSCsz58813

  Symptoms: Cisco UC500 console displays the following log(s) constantly:

  ```
  %PQII_PRO_FE-4-QUEUE_FULL: Ethernet Switch Module transmit queue is full.
  ```

  Phones and hosts connected to the UC can not retrieve IP addresses via DHCP.

  Conditions: This problem occurs shortly after a reload of the Cisco UC500 (on the CME side). This problem is observed after upgrading from Cisco IOS Release 12.4(20)T2 to Cisco IOS Release 12.4(20)T3.

  Workaround: There is no workaround.

- CSCsz63721

  Symptoms: CPU utilization goes to 90% or above when PfR is configured with a large number of policy using fastmode and forced target.

  Conditions: The problem is limited to a large number of forced target (greater than 500) and fastmode with probe frequency of 2-5 seconds. CPU usage progressively gets worse with the increase in number.

  Workaround: Use longest-match targets instead of forced targets. Forced targets are configured under oer-map, and longest-match targets are configured under OER master. Forced targets are required only if the target does not belong to the destination subnet of the traffic-class being optimized.

- CSCsz66965

  Symptoms: After the activation of the HW encryption modules (VSA), the following message is logged by Cisco 7200:

  ```
  %VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption error, Unknown Error
  ```

  There is a traffic impact towards the destination mentioned in the error.

  Conditions: This symptom occurs when VSA hardware encryption is used on a Cisco 7200 with Time-based anti-replay (TBAR) enabled.

  Workaround: Disable Time-based anti-replay (TBAR).

  Further Problem Description: This happens when VSA receives a very small UDP fragment that is less than 26 bytes.

- CSCsz69486

  Symptoms: A multicast video stream forwarded between GE0/0 subinterfaces is policed by the Control Plane Policing (CoPP) class-default. As soon as CoPP is removed, the video recovers its original quality.

  With CEF:

  qffsydbd6ar01#deb control-pl

  qffsydbd6ar01#sh log | i reason

  Control Plane: marking pak exception [cef reason 12]

  Control Plane: marking pak exception [cef reason 39]

  Without CEF:

  qffsydbd6ar01(config)#no ip cef

qffsydbd6ar01#deb control-pl

qffsydbd6ar01#sh log

Control Plane:marking in pak exception [non cef linktype IP]

Conditions: This occurs after upgrading to Cisco IOS Release 12.4(20)T2.

Workaround: There is no workaround.

- CSCsz74859

  Symptoms: NHRP cache entry is not getting created for certain spoke nodes.

  Conditions: This symptom occurs when two spokes A and B advertise the same subnet with varying masks (anything other than /8 or /16 or /24). A third spoke upon receiving such routes (from the hub), in order to send traffic to such subnets, can form a dynamic tunnel with either A or B but not both at the same time.

  Workaround: There is no workaround.

  Further problem description: There is no hindrance to traffic since it continues to flow via the hub. When tunnel with spoke A is formed, there is no problem with traffic to subnet behind spoke A. But, traffic to subnet behind spoke B takes the spoke A - hub - spokeB path. This can be easily noted by traceroute.

- CSCsz79001

  Symptoms: A Cisco 87x router may hang or crash after displaying “Now reloading” during ROMmon upgrade when using the **upgrade rom-monitor file flash:** command.

  Conditions: This occurs when a router running ROMmon release 12.3(8r)YI4 or an older ROMmon from alternate space is upgraded to YI5 or a newer ROMmon version

  Workaround: Powercycle the router to recover from this hang state. The router will then boot with the upgraded ROMmon.

- CSCsz92463

  Symptoms: GetVPN Key Servers no longer function in cooperative mode. The Key Servers (KSs) will fail to communicate with each other, and each will assume it is the primary. GMs registering to different KSs will not be able to communicate with GMs registered to a different KS.

  Conditions: This symptom occurs when using GetVPN Key Servers in cooperative mode.

  Workaround: There is no workaround.

- CSCsz92924

  Symptoms: CPU HOG in Crypto ACL is seen on the GM. The GM may crash some milliseconds later after printing the hog.

  Conditions: This symptom is observed on a large ACL on the KS (greater than 70 lines) with or without large ACL locally on the GM.

  Workaround: Limit the ACL length drastically.

Resolved Caveats—Cisco IOS Release 12.4(22)T1

Cisco IOS Release 12.4(22)T1 is a rebuild release for Cisco IOS Release 12.4(22)T. The caveats in this section are resolved in Cisco IOS Release 12.4(22)T1 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCeg87070

  Symptoms: A Cisco 10000 crashes at the igmp-process:

  ```
  Cisco IOS Software, 10000 Software (C10K2-P11-M), Version 12.3(7)XI2b, RELEASE
  SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c)
  1986-2005 by Cisco Systems, Inc. Compiled Sat 08-Jan-05 16:25 by <software engineer>
  ROM: System Bootstrap, Version 12.0(20020314:211744) [REL-pulsar_sx.ios- rommon 112],
  DEVELOPMENT SOFTWARE
  r-pa068 uptime is 19 hours, 58 minutes System returned to ROM by RPR switchover at
  19:03:47 MET Mon Jan 24 2005 System restarted at 19:07:22 MET Mon Jan 24 2005 System
  image file is "disk0:c10k2-p11-mz.123-7.XI2b"
  ```

  Conditions: This symptom is observed during 7xi2b monitoring.

  Workaround: There is no workaround.

- CSCek75694

  Symptoms: A router that is running Cisco IOS Release 12.4T may reload unexpectedly.

  Conditions: Occurs when BFD is configured and active.

  Workaround: Disable the BFD feature.

- CSCsc78999

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

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

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

- CSCsd35958

  Symptoms: A Cisco 7304 that is configured with an NPE-G100 processor and ATM VCs may reload unexpectedly.

  Conditions: This symptom is observed when a hierarchical policy on an ATM VC has the **shape average** command enabled.

  Workaround: Do not use a hierarchical policy on an ATM VC.

- CSCse26506

  Symptoms: When you perform an OIR of an ATM line card, a CPUHOG condition may occur in the "BGP Event" process.

  Conditions: This symptom is observed when the ATM line card is configured with about 15,000 /32 routes.

  Workaround: There is no workaround.

  Further Problem Description: The ATM line card connects to about 15,000 different gateways, each of which is covered by its own /32 route. In addition, there is a less specific route that covers everything. The symptom occurs when BGP attempts to remove a large number of these tracked entries without suspending any.

- CSCsg39977

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

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

Workaround: There is no workaround.

- CSCsg84765

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

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

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

  Workaround: There is no workaround.

- CSCsi17158

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

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

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

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

  line vty 0 4 transport input telnet end

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

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

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

  http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

- CSCsi35544

  Symptoms: A router may reload with the message “Unexpected exception to CPU.”

  Conditions: The symptom is observed when EzVPN remote using client mode is configured on the router. It is seen when an IP address is being removed from one of the EzVPN inside interfaces while having active NAT translations.

  Workaround: There is no workaround.

- CSCsi99449

  Symptoms: A traceback is seen.

  Conditions: This symptom is observed when the WLAN feature of NAT is configured and when the host with the static IP address tries to contact any host connected to the outside interface of the NAT.

  Workaround: There is no workaround.

- CSCsj33299

  Symptoms: When performing SSLVPN stress tests, thousands of tracebacks are seen on the console. Sometimes there are so many tracebacks, it is hard to get console access. In addition, after many of these tracebacks are seen, the SSLVPN traffic rate that is maintained by the router drops significantly.

  Conditions: This symptom is observed when performing SSLVPN stress tests.

  Workaround: There is no workaround.

- CSCsj34557

  Symptoms: Router displays following error message and reloads:

  ```
  Jun 18 06:12:23.008: event flooding: code 10 arg0 0 arg1 0 arg2 0
  %SYS-3-OVERRUN: Block overrun at E5D8310 (red zone 00000000) -Traceback= 0x6080CEB0
  0x60982108 0x60982EC0 0x6098511C 0x609853BC %SYS-6-MTRACE: mallocfree: addr, pc
  662B5B1C,608A6F3C 0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 662B5B1C,608A6F3C
  0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 %SYS-6-MTRACE: mallocfree: addr, pc
  662B5B1C,608A6F3C 0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 662B5B1C,608A6F3C
  0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 %SYS-6-BLKINFO: Corrupted redzone blk
  E5D8310, words 6088, alloc 61FE2638, InUse, dealloc 80000000, rfcnt 1 -Traceback=
  0x6080CEB0 0x609681D4 0x6098211C 0x60982EC0 0x6098511C 0x609853BC %SYS-6-MEMDUMP:
  0xE5D8310: 0xAB1234CD 0xFFFE0000 0x0 0x63894208 %SYS-6-MEMDUMP: 0xE5D8320: 0x61FE2638
  0xE5DB2D0 0xE5D8144 0x800017C8 %SYS-6-MEMDUMP: 0xE5D8330: 0x1 0x0 0x1 0x64B53478
  %Software-forced reload
  ```

  Conditions: Occurred on a Cisco 7200 running the c7200-ik9s-mz.124-7a.bin image.

  Workaround: There is no workaround.

- CSCsj36133

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

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

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

- CSCsj97952

  Description: A large file (typically of sizes greater than 60 MB, which we took as a reference to reproduce the problem) that is copied using Windows networking (PC-to-PC drag and drop on a shared drive) across a network can cause unexpected latency for traffic in different QoS classes when the access is via a Cisco 3845 with an NM-1A-OC3-POM interface.

  Symptoms: When a large file is copied using Windows file transfer (best- effort traffic), the priority class traffic gets delayed and sees high latency values (at the maximum, the latency can reach 100 ms with average hovering around 60 ms).

Conditions:

Hardware Configuration: This bug is seen when an NM-1A-OC3-POM card is used for passing the traffic on a low-bandwidth PVC (1-Mbps PVC was used while testing).

Software Configuration: Configure priority EF traffic stream with 30 percent of 1 Mbps reserved and the rest of the bandwidth set aside for best- effort traffic.

Network Conditions: This symptom occurs when a low-bandwidth PVC is configured (less than 10 Mbps) and is due to the bursty nature of best-effort traffic ONLY.

Workaround: This observation is made only when the input best-effort traffic is bursty in nature. Regularized best-effort traffic flow does not seem to affect other priority traffic classes. To eliminate the symptoms, apply input policing to rate-limit best-effort traffic.

- CSCsk41593

  Symptoms: The following error occurs when a ping packet is sent or received:

  ```
  PAK_SUBBLOCK_ALREADY: 2 -Process= "IP Input"
  ```

  Conditions: Occurs when large ping packets (greater than 1500 bytes) are sent to back-to-back cellular interfaces with GRE tunneling enabled.

  Workaround: Disable the **ip virtual-reassembly** command on the cellular interface.

- CSCsk98751

  Symptoms: A router may crash after the **mpls traffic-eng backup-path tunnel** command is issued.

  Conditions: The symptom is observed when a backup tunnel is configured on PLR, which is a mid point router for a protected primary tunnel.

  Workaround: There is no workaround.

- CSCsl00472

  Symptoms: A Cisco router unexpectedly reloads with memory corruption after showing multiple "%SYS-2-INPUT_GETBUF: Bad getbuffer" messages.

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCsl46159

  Symptoms: When the cost-minimization feature is used in OER, prefixes are moved to minimize the cost, but it never reaches a stable point. In other words, prefixes are moved back and forth periodically.

  Conditions: This symptom is observed only if OER cost-minimization is configured.

  Workaround: There is no workaround.

- CSCsm01389

  Symptoms: Crash occurs after clearing auto-tunnel backup by issuing the **clear mpls traf-eng auto-tunnel backup** command.

  Conditions: Occurs with SSO and traffic engineering (TE) auto-tunnel feature enabled.

  Workaround: There is no workaround.

  Further Problem Description: Crash was seen on Active SP after issuing the **clear mpls tra auto-tunnel primary** command followed by the **clear mpls tra auto-tunnel backup** command. This crash could happen with or without an SSO switchover before issuing those commands.

- CSCsm03452

  Symptoms: A Cisco AS5850 that is configured as a SIP gateway may crash unexpectedly when running a high volume of SIP calls.

  Conditions: This symptom is observed on the Cisco AS5850.

  Workaround: There is no workaround.

- CSCsm83996

  Symptoms: GM encrypts packets that match GMACL deny.

  Conditions: This symptom is observed when the GMACL is configured on the highest priority crypto map.

  Workaround: Configure the GMACL on a lesser priority crypto map.

- CSCsm92992

  Symptoms: Brand new NVRAM chips will not have the magic numbers written for the primary, backup, and secondary backup NVRAM. This will cause error messages when trying to read/write to the NVRAM (see below).

```
Router# write erase
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
Router#
*Dec 17 23:08:52.319: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvramwr
Building configuration...
[OK]
Bad configuration memory structure -- try rewriting
Bad configuration memory structure -- try rewriting
Router#
Router#
Router# wr
Bad configuration memory structure -- try rewriting
Bad configuration memory structure -- try rewriting
Building configuration...
[OK]
Bad configuration memory structure -- try rewriting
Bad configuration memory structure -- try rewriting
Router#
```

  Workaround: Load an image older than Cisco IOS Release 12.4(20)T, which will write the magic numbers. Then load an image from Cisco IOS Release 12.4(20)T or a later release.

- CSCso67195

  Symptoms: A router may crash due to memory corruption:

```
*Apr 7 12:32:14: %SEC-6-IPACCESSLOGRP: list 111 denied pim 0.0.0.0 -> <removed>, 1
packet
*Apr 7 12:32:29: %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk
680A5374 data 680A79A4 chunkmagic FFFFFFFF chunk_freemagic 0 - Process= "Mwheel
Process", ipl= 0, pid= 274, -Traceback= 0x6169C450 0x60102E78 0x601031E4 0x61D418E4
0x61D4230C 0x61CF1A48 0x61D1280C 0x61D05FE4 0x61D0E9FC
chunk_diagnose, code = 1
chunk name is PIM JP GroupQ
```

  Conditions: This symptom occurs when PIM is enabled on an interface and access-list logging is enabled.

  ip pim sparse-dense-mode
  access-list 98 deny any log

Workaround: Remove access-list logging.

- CSCsq03005

  Symptoms: Fax fails when the **supervisory disconnect** command is applied on a voice port. The default fax detect script, app_fax_detect.2.1.2.2.tcl, is being used.

  voice-port 2/0/20
  supervisory disconnect dualtone mid-call

  When the **supervisory disconnect dualtone mid-call** command is removed, fax works.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T4.

  Workaround: There is no workaround.

- CSCsq13938

  Symptoms: In Cisco IOS software that is running the Border Gateway Protocol (BGP), the router may reload if BGP **show** commands are executed while the BGP configuration is being removed.

  Conditions: This problem may happen only if the BGP **show** command is started and suspended by auto-more before the BGP-related configuration is removed, and if the BGP **show** command is continued (for example by pressing the SPACE bar) after the configuration has been removed. This bug affects BGP **show** commands related to VPNv4 address family. In each case the problem only happens if the deconfiguration removes objects that are being utilized by the **show** command. Removing unrelated BGP configuration has no effect.

  This bug is specific to MPLS-VPN scenarios (CSCsj22187 fixes this issue for other address-families).

  Workaround: Terminate any paused BGP **show** commands before beginning operations to remove BGP-related configuration. Pressing “q” to abort suspended show commands, rather SPACE to continue them, may avoid problems in some scenarios.

- CSCsq23391

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

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

  Workaround: There is no workaround.

- CSCsq29139

  Symptoms: When IPv6 prefix delegation receives periodic RENEW message from a client, it may incorrectly bind the corresponding prefix for another client.

  Conditions: The symptom is observed when IPv6 prefix delegation assigns a prefix to a client that is connected via a virtual access interface.

  Workaround: There is no workaround.

- CSCsq44792

  Symptoms: Per session queuing does not work with PPPoE session.

  Conditions: Occurs on a Cisco router configured for Mobile Ad Hoc Networks (MANET).

  Workaround: There is no workaround.

- CSCsq50977

  Symptoms: Trimble Palisade NTP Synchronization Driver feature does not work.

  Conditions: Occurs on a Cisco 7200 NPE-G2 running Cisco IOS Release 12.4(15)T3 and 12.4(15)T5. Issue is not seen on NPE-400 running Cisco IOS Release 12.4(15)T3 and 12.4(15)T5.

Workaround: There is no workaround.

- CSCsq57731

  Symptoms: A router that is configured with QoS + Firewall may crash while the **service-policy** command is unconfigured from a tunnel interface.

  Conditions: This symptom is observed when a zone-base firewall is configured along with QoS and when an attempt is made to remove the QoS **service- policy** command from a GRE tunnel interface.

  Workaround: There is no workaround.

- CSCsq73501

  Symptoms: Unable to create sessions and ACLs.

  Conditions: The symptom is observed when testing with DACL.

  Workaround: There is no workaround.

- CSCsq92019

  Symptoms: An SCCP phone cannot act as a conferencing controller.

  Conditions: This symptom is specific to a customer test setup where there is NAT back-to-back. NAT segmented code synchronization fails when NAT is back-to-back.

  Workaround: Configure the **no ip nat service skinny tcp port 2000** command.

- CSCsq92440

  Symptoms: A router may crash when continuously executing the **sh ip mroute count | incl groups** command with large number of mroutes.

  Conditions: The symptom is observed only when unconfiguring a large number of static joins at a time or unconfiguring the class-map having large number of groups and executing the **sh ip mroute count | incl groups** command multiple times continuously. (Unconfiguration/configuration of a large number of static joins can be done only by using a class-map.)

  Workaround: Do not check **sh ip mroute count | incl groups** continuously when unconfiguring or configuring a large number of mroutes.

- CSCsq97517

  Symptoms: On a newly-rebooted router, CEF states on SP will not be in sync with RP.

  Conditions: It is a very rare race condition that triggers this problem. It is not seen on many platforms.

  Workaround: There is no workaround, other than reloading the router.

- CSCsq98742

  Symptoms: Cisco AS5400 router crashes frequently with Cisco IOS Release 12.4(19b) attempting to free memory for X28 component.

  Conditions: This symptom is observed on a Cisco AS5400.

  Workaround: There is no workaround.

- CSCsr18691

  Cisco IOS devices that are configured with Cisco IOS Zone-Based Policy Firewall Session Initiation Protocol (SIP) inspection are vulnerable to denial of service (DoS) attacks when processing a specific SIP transit packet. Exploitation of the vulnerability could result in a reload of the affected device.

  Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available within the workarounds section of the posted advisory.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090923-ios-fw.shtml

- CSCsr24551

  Symptoms: A Cisco 7200 VXR series router may crash and reload upon applying a policy map.

  Conditions: This symptom is observed when the service policy map is applied on the channelized E3 interface of a Cisco 7200 VXR router and traffic is pumped. The issue is observed only for E3 interface.

  Workaround: Remove the service policy map.

- CSCsr25788

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

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

  Workaround: There is no workaround.

- CSCsr27794

  Symptoms: BGP does not generate updates for certain peers.

  Conditions: BGP peers show a neighbor version of 0 and their update groups as converged. Out queues for BGP peers are not getting flushed if they have connection resets.

  Workaround: There is no workaround other than entering the **clear ip bgp *** command.

- CSCsr29691

  Port Address Translation (PAT) is a form of Network Address Translation (NAT) that allows multiple hosts in a private network to access a public network using a single, public IP address. This is accomplished by rewriting layer 4 information, specifically TCP and UDP source port numbers and checksums, as packets from the private network traverse a network device that is performing PAT. PAT is configured by network administrators and performed by network devices such as firewalls and routers in situations where public IP addresses are limited.

  After the initial multi-vendor DNS advisory was published on July 8th, 2008, it was discovered that in some cases the fixes to DNS implementations to use random source ports when sending DNS queries could be negated when such queries traverse PAT devices. The reason for this is that in these cases the network device performing PAT uses a predictable source port allocation policy, such as incremental allocation, when performing the layer 4 rewrite operation that is necessary for PAT. Under this scenario, the fixes made by DNS vendors can be greatly diminished because, while DNS queries seen on the inside network have random source port numbers, the same queries have potentially predictable source port numbers when they leave the private network, depending on the type of traffic that transits through the device.

  Several Cisco products are affected by this issue, and if DNS servers are deployed behind one of these affected products operating in PAT mode then the DNS infrastructure may still be at risk even if source port randomization updates have been applied to the DNS servers.

  This bug is for Cisco IOS software, which may an incremental source port allocation policy when performing the source port rewrite operation that is needed for PAT. Refer to the following URL for information on when the PAT implementation in Cisco IOS will use an incremental port allocation policy:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6640/product_data_sheet0900aecd8064c999.html

(paragraph immediately following the 1st image)

Note that traditional NAT, i.e. allocating one public IP address for each private IP address, is not affected by this problem because, unlike PAT, NAT only rewrites layer 3 information and does not modify layer 4 header information of packets traversing the NAT device.

For more information about the DNS vulnerability mentioned above please refer to the multi-vendor advisory at:

http://www.kb.cert.org/vuls/id/800113

or at the Cisco-specific advisory at:

http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml

- CSCsr37296

  Symptoms: MPLS packets with experimental bit set are not classified according to output service-policy rules.

  Conditions: Occurs when you define an output policy to classify packets by “mpls experimental” bits on output to Multilink:

  class-map match-any *xclass*

  match mpls experimental topmost *5*

  policy-map *xpolicy*

  class *xclass*

  priority percent *99*

  class class-default

  bandwidth percent *1*

  interface Multilink1 service-policy output *xpolicy*

  Workaround: There is no workaround.

- CSCsr39340

  Symptoms: Packets may be dropped.

  Conditions: This symptom is observed if the core interface for AToM is a GRE tunnel.

  Workaround: There is no workaround.

- CSCsr40433

  Symptoms: Traffic engineering (TE) tunnel reoptimization fails and tunnel stuck in “RSVP signaling proceeding”.

  Conditions: Occurs when explicit path with loose next hops and one of the next hops is still reachable and that next hops is a dead-end.

  Workaround: Use strict next hop addresses.

- CSCsr48677

  Symptoms: There may be memory allocation errors and traceback for the Net Background process when HWIC-1FE/2FE is present in the router.

  Conditions: The symptoms are observed when the line protocol state of Fast Ethernet interface in HWIC-1FE/2FE is down for more than 48 hours.

  Workaround: Configure the **no keepalive** command on the interface that is down.

- CSCsr50834

  Symptoms: A CPU hog may be seen after changing the “logging buffered” setting to up to 50 MB or more. This issue can cause an OSPF flap.

  Conditions: The symptoms are observed with Cisco IOS Release 12.2(33)SXH2 on a Cisco WS-C6506.

  Workaround: Instead of manipulating such a large logging buffer at runtime when the device/network is busy, consider configuring the “logging buffered” setting once and save it as part of the startup configuration. This way, the huge logging buffer will be allocated during the device initialization without runtime impact.

- CSCsr54170

  Symptoms: A router may crash when removing policy-map configuration with policy-map still in use (with traffic through).

  Conditions: The symptom is observed if a policy-map is removed from configuration and that policy-map is still referenced by an interface service-policy statement (with traffic through).

  Workaround: Stop traffic before removing policies.

- CSCsr58515

  Symptoms: The commands under the submode **dspfarm profile** are not retrofitted, and the default values are not shown.

  Conditions: The symptom is observed with the commands under the submode **dspfarm profile**. When the **show run all** command is executed, the default values are not displayed.

  Workaround: There is no workaround.

- CSCsr62441

  Symptoms: Router is crashing while configuring “connect <word> voice-port 7/0:0 t1 7/0” and tracebacks can be observed.

  Conditions: The symptoms are observed on a Cisco 5400 platform when configuring “connect <word> voice-port 7/0:0 t1 7/0”.

  Workaround: There is no workaround.

- CSCsr65069

  Symptoms: A router reports “%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header” and reloads.

  Conditions: This symptom is observed with Cisco routers that are running Cisco IOS Release 12.4T under an increased traffic load.

  Workaround: There are no known workarounds.

  Further Problem Description: This issue is related to a classification engine in Cisco IOS software. This engine is used by all features that require classification (for example, QoS, NetFlow).

- CSCsr69433

  Symptoms: A router may experience %SYS-3-CPUHOG: errors and then a watchdog crash in the FR LMI process.

  Conditions: The symptoms are observed when ISDN is configured on the router.

  Workaround: There is no workaround.

- CSCsr72352

  Symptoms: EBGP-6PE learned IPv6 labeled routes are advertised to IBGP-6PE neighbor by setting NH as local IP address.

  Conditions: This symptom is observed on 6PE Inter-AS Option C with RR case.

  Workaround: There is no workaround.

- CSCsr82471

  Symptoms: A dial-peer's preference is changed. This problem is observed in any Cisco IOS version since the ephone-hunt secondary preference is supported. The latest images, such as 12.4(20)T1, 12.4(22)T1, and 12.4(22) YB1, also exhibit this issue.

  Conditions: This symptom is observed when ephone-hunt has secondary preference configured.

  Workaround: Remove secondary preference in ephone-hunt.

- CSCsr82895

  Symptoms: When a router has many PPPoE sessions and the router is configured as an RP-mapping agent, the router crashes following a switchover.

  Conditions: The symptom is observed when the router has 8000 PPPoE sessions and it is configured as an RP-mapping agent. Following a switchover, the issue is seen.

  Workaround: Another router that does not have as many interfaces in the network should be configured as the RP-mapping agent.

- CSCsr83547

  Symptoms: Dialer watch on the Cisco 3845 router makes the backup link of PPP multilink on the PRI port which is connected to BRI 4 port of peer router through ISDN net. If one out of four BRI ports is shut down on the peer router, the dialer watch does not keep the backup link up without resetting the idle timer at the expiration of idle timeout though the primary link remains down, causing the other three ports to be disconnected.

  Conditions: This symptom occurs only when the BRI port which contains B-ch that became link up first is shut down. This symptom does not occur even if the other BRI ports are shut down.

  Workaround: There is no workaround.

- CSCsr85757

  Symptoms: IGMPv3 not enabled on VLAN as expected

  Conditions: By default, the **ip igmp snooping** command enables IGMP snooping on a VLAN, but in the failed case, it is not enabled.

  Workaround: There is no workaround.

- CSCsr93764

  Symptoms: Bus error exceptions due to Application Firewall HTTP inspection.

  Conditions: This issue has been seen in several Cisco 3845 routers running Cisco IOS Release 12.4(15)T5 with IP Inspect configured.

  Workaround: There is no workaround.

- CSCsr96042

  Symptoms: A Cisco ASR 1000 router crashes.

  Conditions: Occurs if "ip vrf" is deleted from the configuration.

  Workaround: There is no workaround.

- CSCsr96753

  Symptoms: A router may crash when entering the **isdn test call** command.

  Conditions: The symptom is observed when the BRI interface is up.

  Workaround: There is no workaround.

- CSCsr97343

  Symptoms: An MSDP peer may flap randomly.

  Conditions: The symptom is observed when the device is configured with **logging host** *ip-address ...* or **logging host** *ip-address*.

  Workaround: It has been observed that removing the "logging host" configuration helps in preventing the peer-flap:

  no logging host *ip-address* **no logging** *ip-address*

- 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.

- CSCsu00266

  Symptoms: The following crash is observed after configuring a policy-map.

  ```
  SegV exception, PC 0x2142818 at 10:04:23
  ```

  Conditions: Occurred on a Cisco 7206VXR (NPE-G2) running Cisco IOS Release 12.4(15)T5.

  Workaround: There is no workaround.

- CSCsu03038

  Symptoms: A memory leak occurs.

  Conditions: This symptom is observed in some cases when SSG TCP redirection is used.

  Workaround: There is no workaround.

- CSCsu06350

  Symptoms: T.38 fax call not terminating audio properly.

  Conditions: RE-INVITE from SIP Fax application changes connection IP address in SDP. PGW sends changed IP address in MDCX to GW. GW responds with 200 acknowledging this change. GW still sends audio to IP address where original call terminated.

  Workaround: There is no workaround.

- CSCsu08935

  Symptoms: BGP as-override does not work properly on a PE to overwrite the AS in the AS4_PATH.

  Conditions: When a 4-byte CE is peered to a 2-byte-capable PE using AS 23456 and the **as-override** command is configured on the neighbor, the PE router does not override the AS in the AS4_PATH with its own AS number, mapped to 4 bytes.

  Workaround: Use "allowas-in" on the CE.

- CSCsu10229

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

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

  Workaround: There is no workaround.

- CSCsu12040

  Symptoms: BGP neighbors that are configured with as-override and send-label (CsC) together may not work after an interface flap or service reset.

  Conditions:

  neighbor xxx as-override
  neighbor xxx send-label

  Workaround: Enter the **clear ip bgp * soft in** command.

  Further Problem Description: Peers (neighbors) with a CsC (IPv4+label) BGP configuration with the as-override option should be separated into different dynamic update groups during the BGP update generation process. After the CSCef70161 fix in Cisco IOS Release 12.0(32)SY4, this is no longer the case; this CSCsu12040 fix enhances the CSCef70161 fix to handle the CsC (IPv4+label) case separately.

- CSCsu18232

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

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

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

- CSCsu20411

  Symptoms: A router may crash while unconfiguring “source template test” in interface configuration mode.

  Conditions: The symptom is observed with a router loaded with Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsu21828

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

  Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

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

- CSCsu23940

  Symptoms: The error message “Must remove traffic-shape configuration first” is seen, and QoS policy is not getting attached.

  Conditions: This symptom is seen when unable to attach a queuing policy-map (“bandwidth” configured) through Frame-relay (FR) map-class to a FR-DLCI interface with FRTS enabled.

  Workaround: There is no workaround.

  Further Problem Description: This has a major functional impact as the QoS- Policy is not getting attached.

- CSCsu24505

  Cisco IOS Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available and are documented in the workarounds section of the posted advisory.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml

- CSCsu25797

  Symptoms: When the router is running with an on-board VPN module, the module driver should update the maximum IKE SA limit to support more tunnels than software encryption. However, the on-board driver may not update the limit when Cisco IOS Release 12.4(11)T or later is used. Therefore, only 100 IKE SA are supported with the on-board module.

  Conditions: The symptom is observed with a Cisco 2811 or 2821 router that is running Cisco IOS Release 12.4(11)T or a later release.

  Workaround: Use Cisco IOS Release 12.4(9)T.

- CSCsu25833

  Symptoms: An ISR router may crash with the following error message:

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

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

  Workaround: There is no workaround.

- CSCsu26174

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

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

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

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

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

- CSCsu26526

  Symptoms: Memory leak can be seen on the LNS.

Conditions: The symptom is observed on the L2TP Network Server (LNS) when the PPP client does a renegotiation.

Workaround: There is no workaround.

- CSCsu27888

  Symptoms: IGMP v3 reports are discarded.

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

  Workaround: There is no workaround.

- CSCsu31444

  Symptoms: A BR continuously displays errors messages on the console.

```
Router#%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
```

  OER jitter probes are not created because of this error.

  Conditions: This symptom is observed with the jitter probe configuration below for VOIP optimization:

```
oer-map BRANCH 20
 match traffic-class access-list Optimize_Voice_Traffic
 set mode route control
 set mode monitor fast
 set resolve mos priority 1 variance 30
 set resolve delay priority 2 variance 30
 set active-probe jitter 10.100.10.1 target-port 1025 codec g729a <<
 set probe frequency 4
```

  Workaround: Set higher probe frequency (higher than 5).

- CSCsu32069

  Symptoms: The router crashes when call-home tries to establish a secure HTTP connection to a server.

  Conditions:

  1. The call-home profile has an HTTP destination address pointing to a secure HTTP server. For example: destination address http https://172.17.46.17/its/service/oddce/services/DDCEService.

  2. When there is no crypto pki trustpoint to be used by secure HTTP connection.

  Workaround: Configure a crypto pki trustpoint to be used by the secure HTTP connection.

  Further Problem Description: The crash is seen only with call-home feature, though the root cause exists in base code.

- CSCsu32154

  Symptoms:

  Calls through an MGCP-controlled FXS may fail to complete. The user will hear fast-busy signal when attempting to make inbound or outbound calls from or to that port. Outbound calls to the port in this state may return a 400 error “Previous message in-progress” in response to the CRCX.

Conditions:

The symptom is observed under rare conditions with an MGCP-controlled FXS port on a Cisco IOS Voice over IP (VoIP) gateway.

To verify that a port is in this state, compare the output of **show mgcp connection** to the output of **show voice call summary**. If a call appears with the mgcp show command output for a port but that port appears idle (FXLS_ONHOOK) in the voice call output, this would indicate the problem being seen.

An example of such output is here showing port 2/1 in this state:

VG224# sh voice call summ

PORT CODEC VAD VTSP STATE VPM STATE ============== ========= === ==========
========== ========== 2/0 - - - FXSLS_ONHOOK 2/1 - - - FXSLS_ONHOOK

VG224# sh mgcp conn

Endpoint Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent [SIFL] (R)esult[EA (ME)dia (COM)Addr:Port 1. aaln/S2/1 C=,34,-1 I=0x0 P=0,0 M=0 S=9,0 CO=0 E=3,10,10,10 R=41,0 ME=0 COM=0.0.0.0:0

Workaround:

Reload the gateway to recover a port once it is in this state. Attempting to restart the MGCP service on the gateway by removing and adding the **mgcp** command in the configuration has been shown at times to be ineffective once in this state.

Alternate workaround: Use of H323/SIP signaling instead of MGCP will prevent ports from getting into this state.

Further Problem Description:

Changes applied through CSCsq97697 have been found to greatly reduce the instances of this issue from occurring. If using H323/SIP instead of MGCP is not an option, it is recommended to use a Cisco IOS Release that contains the changes in CSCsq97697 (for example, Cisco IOS Release 12.4(15)T7).

The changes applied to CSCsu32154 introduce a new MGCP CLI command which is not enabled by default. If upgrading to obtain a fix for this issue, configure **mgcp disconnect-delay**.

- CSCsu32168

  Symptoms: During a manual clear of PPPoE sessions associated with a VMI interface (using the **clear pppoe all** command), the router may crash.

  Conditions: The symptom is observed when sessions are established and all cleared at once. The router will then crash and create a crashinfo file. On a Cisco 3200 series router, the router may hang. When the 3200 series router hangs, the router console becomes unresponsive.

  Workaround: There is no workaround. When the Cisco 3200 series router hangs the hung condition may be cleared by sending a break to the console or by power cycling the router.

- CSCsu33111

  Symptoms: The **shutdown** command is not working as expected and it reloads the NME-16ES-1G Service Module instead.

  Conditions: When the **service-module gigabitEthernet <x/y> shutdown** command is issued from ISR, the NME-16ES-1G Service Module reloads instead of shutting down.

  Workaround: There is no workaround.

- CSCsu35597

  Symptoms: Renaming a directory gives error message.

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

  Workaround: There is no workaround.

- CSCsu35776

  Symptoms: When running zone-based firewall (ZBF), there is a memory leak in the Chunk Manager.

  Conditions: When viewing the memory information with **show processor memory** command, the Chunk Manager process will grow continuously as long as traffic is running. Eventually all memory will be exhausted.

  Workaround: There is no workaround.

- CSCsu39338

  Symptoms: Redistributed routes are not removed even though network is down. Redistribution is done between BGP and OSPF.

  Conditions: Occurs on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsu40497

  Symptoms: IPIPGW/CUBE drops the H.245 OpenLogicalChannel(OLC) received from Cisco Voice Portal (CVP). This results in call failure.

  Conditions: This occurs when IPIPGW/CUBE is deployed in H.323-H.323 mode, running Cisco IOS Release 12.4(20)T and registered to a gatekeeper and talking to a CVP server.

  Workaround: Do not register the IPIPGW/CUBE to a Gatekeeper.

- CSCsu42078

  Symptoms: A router may crash due to bus error caused by an illegal access to a low memory address.

  Conditions: This happens when a service-policy is applied to an interface, and then service-policy is removed under certain conditions.

  One such condition is that “ip cef distributed” was configured on the router and the multi-link member flap triggered the service policy removal.

  Workaround: Remove “ip cef distributed” from the configuration.

- CSCsu44789

  Symptoms: Spurious memory access traceback is seen.

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

  Workaround: There is no workaround.

- CSCsu45973

  Symptoms: A router may crash very close in time to when an RFC 4938 compliant PPPoE session is being terminated.

  Conditions: The symptom is observed when the VMI interface is in aggregate mode and an RFC 4938 compliant PPPoE session is terminated.

  Workaround: There is no workaround.

- CSCsu46060

  Symptoms: A router may crash under low memory conditions.

  Conditions: The symptom is observed with a router running GetVPN and Cisco IOS Release 12.4(15)T7.

  Workaround: There is no workaround.

- CSCsu47660

  Symptoms: Line Flaps

  Conditions: The problem is observed on E1 link with HDLC and PPP encapsulation. Cisco Express Forwarding (CEF) is enabled.

  Workaround: Disable CEF.

- CSCsu48898

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

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

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

- CSCsu50873

  Symptoms: The PBR Next Hop Recursive feature does not function unless CEF is disabled on the corresponding interface.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(20)T.

  Workaround: There is no workaround.

- CSCsu54801

  Symptoms: IPv6/IPv6 Tunnel adjacency information is incomplete on the line card. This prevents IPv6/IPv6 multicast traffic on the tunnel.

  Conditions: The symptoms are observed under normal operation.

  Workaround: There is no workaround.

- CSCsu62667

  Symptoms: LSP ID change after stateful switchover (SSO) due to failure in signaling recovered label switched path (LSP).

  Conditions: Occurs following a SSO switchover.

  Workaround: There is no workaround.

- CSCsu64215

  Symptoms: Router may incorrectly drop non TCP traffic. TFTP and EIGRP traffic can be impacted as seen in CSCsv89579.

  Conditions: Occurs when the **ip tcp adjust-mss** command is configured on the device.

  Workaround: Disable **ip tcp adjust-mss** on all interfaces. Note that this may cause higher CPU due to fragmentation and reassembly in certain tunnel environments where the command is intended to be used.

- CSCsu64323

  Symptoms: The **show vpdn history failure** command should show the history of session failures due to entering incorrect password, but it does not show any history.

  ```
  Router# show vp hi fa
  ```

```
% VPDN user failure table is empty
```

Conditions: The problem was seen with a Cisco 7201 that is running Cisco IOS Release 12.2(33)SRC1. No problem is seen with Cisco IOS Release 12.4(4)XD9.

Workaround: There is no workaround.

- CSCsu65189

  Symptoms: If router is configured as follows:

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

  And later is enabled LDP/IGP synchronization using the command:

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

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

```
Router# sh ip ospf mpls ldp in

Loopback0
  Process ID 1, Area 0
  LDP is not configured through LDP autoconfig
  LDP-IGP Synchronization : Required < ---- NOK
  Holddown timer is not configured
  Interface is up
```

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

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

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

  The problem will not occur if LDP/IGP sync is already in place and:

  - Router is reloaded with image with fix for CSCsk48227.
  - The passive-interface command is removed/added.

- CSCsu65495

  Symptoms: VoIP round trip delay certification test fails in some applications.

  Conditions: Occurs in applications that have strict requirements for round-trip delay times.

  Workaround: There is no workaround.

- CSCsu69750

  Symptoms: MTP is not able to handle G729a codec and G729 codec on both call legs at same time.

  Conditions: The symptoms are observed with Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

  Further Problem Description: If enabling “debug sccp all”, the debug output indicates that it is an “Unsupported mtp req”.

- CSCsu70909

  Symptoms: If an ICMP connection is initiated from outside to a global address of a static NAT translation and zone-based firewall (ZBF) is configured, matching that flow, the resulting echo reply will be denied.

  Conditions: This issue was observed on a Cisco 3845 running Cisco IOS Release 12.4(20)T. ZBF was configured in both directions and a static NAT was involved. The outside host was pinging the global NAT address.

  Workaround: Creating a class-map that matches protocol ICMP and applying that to both inside-to-outside and outside-to-inside policy-maps with a pass allows the traffic to flow.

  Further Problem Description:

```
Inspect
      Number of Half-open Sessions = 1
      Half-open Sessions
        Session 682674E0 (10.2.2.2:8)=>(10.1.1.205:0) icmp SIS_OPENING
          Created 00:00:11, Last heard 00:00:00
          ECHO request
          Bytes sent (initiator:responder) [96:0]
```

  The session is created, but stuck int eh SIS_OPENING status and last heard is the ECHO request. The packet was actually dropped by ZFW. It appears that it did not match the intended class-map and fell to class-default.

```
*Sep 22 22:45:17.707: %FW-6-LOG_SUMMARY: 8 packets were dropped from 10.2.2.2:8 =>
10.1.1.205:0 (target:class)-(outside-to-inside:class-default)
```

  Passing in the class-default class-map in the outside-to-inside policy-map does not allow the traffic to flow. Additionally passing in the class-default class-map in the inside-to-outside policy-map does not allow the traffic to flow.

- CSCsu71728

  Symptoms: A crash may occur while applying QOS under an MFR interface.

  Conditions: The symptoms are observed while applying QOS under an MFR interface on a PA-MC-2T3-EC in L2VPN.

  Workaround: There is no workaround.

- CSCsu71853

  Symptoms: Transfer calls are failing due to the fact that the router does not have anything for Replaces: and Referred-By: fields.

  Conditions: Occurs in routers running Cisco IOS Release 12.4(15)T6 and Cisco IOS Release 12.4(15)T7.

  Workaround: There is no workaround.

- CSCsu73128

  Symptoms: Router crashes.

  Conditions: Occurs when large number of remote end points try to connect to the gateway at the same time. The router may crash if “rsa-sig” is used as authentication method.

  Workaround: There is no workaround.

- CSCsu73970

  Symptoms: Applying a service policy to an outbound interface causes CPUHOG messages of the following nature, and then it triggers a software-forced crash:

```
%SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs (25/1),process
= IP Input.
```

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = IP Input.
%Software-forced reload
Preparing to dump core... *Sep 23 22:44:39.275 AWST: %SYS-3-CPUYLD: Task ran for
(128072)msecs, more than (2000)msecs (25/1),process = IP Input
22:44:42 AWST Tue Sep 23 2008: Breakpoint exception, CPU signal 23, PC = 0x4004FE88
```

Conditions: This symptom is observed when a service policy is applied to an outbound interface. The service policy should have similar ICMP permit statements:

permit icmp any 172.16.156.16 0.0.0.15 echo-reply
permit icmp any 172.16.156.16 0.0.0.15 echo

The hang occurs when both of these statements are configured at the same time.

Workaround: There is no workaround.

- CSCsu76540

  Symptoms: An extension number in an ephone hunt group may not be reached.

  Conditions: The symptom is observed if an ephone in a hunt group (longest- idle) is put on hold by an internal caller. The hunt group will stop trying to hunt this ephone.

  Workaround: Re-configure this ephone hunt group.

  Further Problem Description: When all the ephones in the hunt group are put on hold, this hunt group can not be reached, even when all the ephones are onhook.

- CSCsu76993

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

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

  Workaround: There is no workaround.

- CSCsu77667

  Symptoms: The **time-range** commands used by ACLs no longer work, and the ACL time-range entries show as always active.

  Conditions: Configure ACL time-ranges and have Cisco IOS code that supports SSLVPN. Once the router is reloaded, SSLVPN takes over the ACL time-ranges and these time ranges no longer work for ACLs.

  Workaround: Reconfigure the configuration mode ACL time-ranges after the reboot.

  Further Problem Description:

  The **show startup-config** command will show the correct configuration:

```
webvpn context Default_context
 ssl authenticate verify all
!
 no inservice
!
time-range afternoon
 periodic weekdays 12:00 to 16:59
```

  With the **time-range** command in global context.

  The **show running-config** command will show the incorrect configuration:

```
webvpn context Default_context
 ssl authenticate verify all
!
 time-range “afternoon”
  periodic weekdays 12:00 to 16:59
```

```
!
 no inservice
!
```

With the **time-range** command in webvpn context.

- CSCsu78553

  Symptoms: Spurious memory found in sslvpn_create_session procedure.

  Conditions: The symptom is observed when SSLVPN is configured.

  Workaround: There is no workaround.

- CSCsu79847

  Symptoms: Memory leak occurs.

  Conditions: Occurs when the **ip access-list logging hash-generation** command is entered.

  Workaround: There is no workaround.

- CSCsu92432

  Symptoms: The router's async line used for reverse SSHv2 might hang after a failed authentication and not recover unless the router is rebooted. The router log displays:

  ```
  %SYS-3-HARIKARI: Process SSH Process top-level routine exited
  ```

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

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

- CSCsu95319

  Symptoms: Igmp-proxy reports for some of the groups are not forwarded to the helper. This causes members not to receive the multicast traffic for those groups.

  Conditions: The problem is seen when the igmp-proxy router is receiving UDP control traffic. That is, the router is receiving any UDP control-plane traffic on any interface.

  Workaround: There is no workaround.

- CSCsu97177

  Symptoms: Device may reload while querying the CISCO-IETF-IP-FORWARD (IPv6) MIB.

  Conditions: SNMP must be configured on the device, and the querier must be aware of the appropriate community to use. Further, there must exist multiple IPv6 global routing tables on the device. This will only be the case if VRFs have been configured with the **vrf definition** command, and that vrf has the IPv6 address family configured, and if that VRF is applied to an interface and global IPv6 addresses configured. This can be confirmed by the existence of multiple tables marked "global" in the output of the **show ipv6 table** command.

  Workaround: Exclude the CISCO-IETF-IP-FORWARD from queries.

  Further problem description: Ensure that SNMP is configured so that it can be accessed only by authorized users.

- CSCsu97507

  Symptoms: After removing one of the "ip name-server xxxx" entries, the **show ip dns view** command displays broken output.

  Conditions: The symptoms are observed with the following steps:

  1. Add several "ip name-server xxxx".

  2. Remove one of the middle entries.

3. Use the **show ip dns view** command.

Workaround: There is no workaround.

Further Problem Description: This issue has been recreated with Cisco IOS Releases 12.4(15)T5, 12.4(15)T7, and 12.4(20)T.

- CSCsu97934

  Symptoms: NPE-G1 is crashing with “pppoe_sss_holdq_enqueue” as one of the last functions.

  Conditions: Unknown.

  Workaround: Entering the **deb pppoe error** command will stop the crashing.

- CSCsv00168

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

  Conditions: The symptoms are observed with Cisco IOS Release 12.4(23.2)T.

  Workaround: There is no workaround.

  Further Problem Description: The CLI function is not affected by the junk values.

- CSCsv00959

  Symptoms: A crash occurs.

  Conditions: This symptom is observed after IPv6 unicast routing is unconfigured and only when EIGRPv6 is configured.

  Workaround: There is no workaround.

- CSCsv01474

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

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

  1. The interface flaps.

  2. The **clear ip route** command is issued.

  3. The **no network <prefix>** command and then the **network <prefix>** command are issued for the network corresponding to the interface.

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

- CSCsv01931

  Symptoms: SSLVPN logins from test tool are unsuccessful. The **show crypto eng acc stat** command displays a large number of API request errors.

  Conditions: This happens when using the hardware crypto engine on a Cisco 1811 router.

  Workaround: Disable the hardware crypto engine and use the software crypto engine.

- CSCsv04275

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

  ```
  <date>: %ATM_AIM-5-CELL_ALARM_UP: Interface ATM<if ID> lost cell delineation. <date>:
  %ATM_AIM-5-CELL_ALARM_DOWN: Interface ATM<if ID> regained cell delineation.
  ```
  The link may go down and then recover automatically.

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

Workaround: There is no workaround.

- CSCsv04674

  Symptoms: The M(andatory)-Bit is not set in Random Vector AVP, which is a must according to RFC2661.

  Conditions: This symptom is observed with Egress ICCN packet with Random Vector AVP during session establishment.

  Workaround: There is no workaround.

- CSCsv04733

  Symptoms: A LAC might terminate a tunnel unexpectedly.

  Conditions: This symptom is seen when the tunnel password exceeds 31 characters.

  Workaround: Use a shorter password if policy allows.

  Further Problem Description: This is seen with Cisco IOS interim Release 12.2 (34.1.3)SB1. With a customer specific special based on Cisco IOS Release 12.2 (31)SB11, it allowed 64 characters.

- CSCsv04836

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

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

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

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

- CSCsv06608

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

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

  Workaround: There is no workaround.

- CSCsv11142

  Symptoms: A call is disconnected during call resume in a sip-h323 call.

  Conditions: This symptom is observed under the following conditions:

  1) Call was held with ReInvite->ECS.

  2) Received call resume ReInvite.

  3) Capabilities exchanged on H323 leg.

  4) Sent OLC.

  5) Upon receiving OLCAck, CUBE should send ReInvite on the SIP leg; instead it sends 200OK.

  Workaround: There is no workaround.

- CSCsv12795

  Symptoms: Control Plane Policing (CoPP) is not matching or policing ICMP packets correctly.

  Conditions: This symptom is observed with routers that are configured with DMVPN and that are running Cisco IOS Release 12.4(15.3)T (or a later release).

  Workaround: There is no workaround.

- CSCsv13562

  Symptoms: A router crashes because of double free scenarios. While handling a 302 response, "ccb->call_info.origRedirectNumber" attempts a double free because of signaling forking. The following message appears in the crashinfo file:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (2/1),process =
  CCSIP_SPI_CONTROL.
  ```

  Conditions: This symptom is observed when Call Manager Express is running.

  Workaround: There is no workaround.

- CSCsv13738

  Symptoms: There are two ways to define VRFs when supporting the 6VPE feature:

  1) ip vrf

  2) vrf definition

  The "vrf definition" configuration may take a much longer time to allow convergence between the PE and the CE than the "ip vrf" configuration.

  Conditions: The symptoms are observed under the following conditions:

  - When the router boots up; and
  - When the issue has been seen using the "vrf definition" configuration; and
  - When the router has over 100,000 VPNv4 BGP routes; and
  - When a large number of VRFs are configured

  Workaround: Use the "ip vrf" configuration, if you have only IPv4 VRFs configured.

- CSCsv14530

  Symptoms: This issue happens when anyconnect vpn client is used in standalone mode to connect to the vpn gateway. Whenever a new session with this vpn client is established, it requests a set of files that are served by the gateway. While serving these files, a leak happens.

  Conditions: This leak has been observed on a Cisco 2811 that is running Cisco IOS Release 12.4(20)T and whenever a standalone anyconnect client is used to establish the session.

  Workaround: Use anyconnect web install.

- CSCsv14826

  Symptoms: An EasyVPN tunnel may get stuck in an IPSEC_Active state after a dialer interface flap. The ISAKMP SA can get stuck in Config_XAuth state after the dialer interface flaps: **show crypto isakmp sa** IPv4 Crypto ISAKMP SA dst src state conn-id slot status 10.10.10.10 10.10.10.11 CONF_XAUTH 2090 0 ACTIVE

  Conditions: The symptoms are observed when EasyVPN is configured on a router and where a dialer interface flaps often.

  Workaround: There is no workaround.

- CSCsv15266

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

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

  ```
  %SYS-6-BLKINFO: Corrupted magic value in in-use block blk XXXXXXXX, words XX, alloc
  XXXXXXXX, Free, dealloc XXXXXXXX, rfcnt X
  ```
  Conditions: The reset is triggered by a configuration change tied to QoS and has been seen while changing one of the following:

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

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

- CSCsv17370

  Symptoms: Some applications do not work properly when VSA is used as the crypto engine in the hub router. In the trace, you might observe TCP checksum corruption. This is not true in all cases. However, it might be a symptom if in the sniffer trace taken on the application client server, the last packet received before terminating the application is around 56 to 64 bytes.

  Conditions: This symptom might happen in a very specific scenario. As a condition, you need to have a VSA on the hub router, and the client and server application needs to be in two different remote locations connected via a VPN tunnel through the hub. In addition, the issue has been verified with a tunnel that is configured with a static crypto map. This issue has also been verified with Fast Ethernet ports only.

  Workaround: Disable the crypto engine or use VAM2+.

- CSCsv20058

  Symptoms: Upon digit_end on the RFC-2833 side, the IPIP GW misinterprets this and sends out h245-alphanumeric, which is duplicate. Typically, the IPIP GW should ignore all the tone packets after the digit_begin is detected until the digit_end.

  Conditions: RTP-NTE to H245-Alphanumeric conversion is triggering this event.

  Workaround: There is no workaround.

- CSCsv21930

  Symptoms: The Embedded Event Manager is not available in the Cisco 860 platforms.

  Conditions: Customers that are running the Cisco 860 platform will not be able to use the Embedded Event manager, which includes the “event manager ...” configuration commands.

  Workaround: There is no workaround.

- CSCsv23797

  Symptoms: A Cisco ASR router goes down.

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

  Workaround: Use regular SCP.

- CSCsv24742

  Symptoms: A Cisco router may report exit link out of policy (OOP) when the 32- bit interface utilization counter wraps. At 100 Mbps traffic rate, this can happen once every 6 minutes.

  Conditions: The symptom is observed on a Cisco router running Performance Routing (PfR) and when the 32-bit interface utilization counter wraps.

  Workaround: There is no workaround.

- CSCsv28806

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

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

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

- CSCsv30075

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

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

  Workaround: There is no workaround.

- CSCsv31812

  Symptoms: Version: disk2:c7200-adventerprisek9-mz.124-22.T on KSs and GMs:

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

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

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

  Workaround: There is no workaround.

- CSCsv38166

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

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

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

Cisco has released free software updates that address this vulnerability.

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

This advisory is posted at the following link:

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

- CSCsv40178

  Symptoms: DMVPN setup, where originally the hub and all the spokes were running Cisco IOS Release 12.4(15)T. CDP is enabled on the tunnel interfaces, and the hub was able to see all the spokes as "CDP neighbor." The customer upgraded a few spokes to Cisco IOS Release 12.4(20)T, after which these spokes were no longer seen as CDP neighbors. The other spokes that were running Cisco IOS Release 12.4(15)T were still seen as CDP neighbors.

  Conditions: This symptom is observed under the following conditions:

  – DMVPN network tunnels configured as mGRE.
  – CDP enabled in the tunnel interface.
  – Running new Cisco IOS Release 12.4(2x)Tx image.
  – Crypto enabled or disabled in the tunnel interface.

  Workaround: Downgrade to Cisco IOS Release 12.4(15)Tx. It is not affected.

  It works fine if running a new Cisco IOS Release 12.4(2x)Tx image and using point-to-point GRE in the tunnel interface.

- CSCsv40404

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

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

  Workaround: There is no workaround.

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

- CSCsv40924

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

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

  Workaround:

  1) Configure the **no-payload** command for the NAT translation. This will stop the corruption, but will also cause all deep packet NATing to stop, which can cause other issues.

  2) Use a port other than 554 for the RTSP steam. This will stop the corruption, but will also stop the router from NATing the embedded IP addresses in the RTSP packets. Depending on the specific implementation of RTSP, this may or may not stop the stream from working.

  3) Change your NAT translation such that the private and public IP addresses have the same number of characters. For instance 192.168.0.1 has 11 characters, and 172.16.100.200 has 14 characters.

- CSCsv42721

  Symptoms: Test device that is configured as AP with EAP-FAST configurations fails to associate with the PC client (with appropriate profiles in place). The **show dot11 assoc** command output shows that state is stuck at “AAA_Auth”.

  Conditions: Association fails between with test device and PC client with EAP-TLS configurations.

  Workaround: There is no workaround.

- CSCsv43385

  Symptoms: Connectivity from a Dynamic Multipoint VPN (DMVPN) hub router to spokes may be lost due to a invalid Cisco Express Forwarding (CEF) adjacency.

  If tunnel protection is configured on the hub, the traffic from hub to spokes will get dropped on the tunnel interface and the **show interface tunnelx** command will show the “Total output drops” counter incrementing.

  This is intermittent and the problem will generally appear right after a reload of the router. It may not happen after some reloads of the router.

  Conditions: Seen only on Cisco IOS Release 12.4(20)T and 12.4(22)T.

  Workaround #1: Disable/enable the tunnel mode:

  interface Tunnel30
  no tunnel mode gre multipoint
  tunnel mode gre multipoint

  Workaround #2: Remove the tunnel configuration and re-add it:

  no interface Tunnel30
  interface Tunnel30
  ip address 192.168.50.1 255.255.255.0
  ip nhrp authentication cisco
  ip nhrp map multicast dynamic
  ip nhrp network-id 111
  ip nhrp holdtime 900
  tunnel source FastEthernet0/0
  tunnel mode gre multipoint

- CSCsv43444

  Symptoms: A router will run out of memory when SIP phones register.

  Conditions: Occurs when Cisco 3911 phones are installed

  Workaround: Disable MWI.

- CSCsv43658

  Symptoms: When a service-policy which is already in use by PDPs of an APN is applied to another APN, the Gateway Support Node (GGSN) to crash.

  Conditions: Occurs when the same service-policy is applied to different APNs.

  Workaround: Apply unique service-policies to each APN. For example if service-policy ggsn1 is applied to apn1.com, then service-policy ggsn2 should be applied to apn2.

- CSCsv45669

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

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

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

- CSCsv46240

  Symptoms: A flow exporter that is configured for v9 may export corrupt data.

  Conditions: This symptom occurs under the following configuration sequence:

  - Create a flow exporter, but do not set any values within the exporter.
  - Create a flow monitor, and apply the exporter to it.
  - Apply the flow monitor to an interface.
  - Configure the destination of the exporter.

  Workaround: Configure the destination of the exporter before applying it to any flow monitors. Alternatively, remove the flow monitor from all interfaces and reapply it, which causes correct export packets to be sent.

- CSCsv48296

  Symptoms: The router reloads with the following error:

  ```
  SYS-6-BLKINFO: Corrupted redzone blk
  ```

  Conditions: Occurs when the **cns image** is active, and a CNS image operation is in progress.

  Workaround: There is no workaround.

- CSCsv49359

  Symptoms: In a scenario where a Cisco 7200 with NPE-400 is used to terminate AnyConnect clients on one side and MPLS VPN on another side, the return packets are never forwarded to the client and tracebacks are produced for every single packet.

  Conditions: Occurs with the following configuration:

  - Full SSL tunnel on one end
  - Packets coming as MPLS labeled packets
  - Cisco 7200 with NPE-400

  Workaround: There is no workaround.

- CSCsv49731

  Symptoms: Cisco IOS automatically adds the violate-action to the configuration when policing traffic.

  For instance, the intended config is as follows:

  policy-map p1
  class c1
  police 20000 4470 conform-action transmit exceed-action set-clp-transmit

  Instead the IOS additionally configures the violate-action on its own as follows:

policy-map p1
class c1
police 20000 4470 conform-action transmit exceed-action set-clp-transmit
violate-action set-clp-transmit

This causes the counters to count the number of exceeded/violated packets incorrectly.

Conditions: This condition occurs in QoS configuration. Occurs on routers running Cisco IOS Release 12.4(20)T1. It was observed across all fixed and modular platforms.

Workaround: There is no workaround.

- CSCsv50666

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

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

  Workaround: There is no workaround.

- CSCsv50958

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

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

  Workaround: No workaround is known.

- CSCsv51021

  Symptoms: Router reloads while trying to ping end-points.

  Conditions: Occurs between end-points through MGRE+IPSEC tunnel.

  Workaround: There is no workaround.

- CSCsv52459

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

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

  Workaround: There is no workaround.

- CSCsv54130

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

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

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

  Then the configuration is changed to Async mode:

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

```
encapsulation slip
async mode dedicated
end
```

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

- CSCsv58256

  Symptoms: When a secure call is put on hold and resumed, the call continues as non-secure call.

  Conditions: Occurs when a secure call is put on hold.

  Workaround: There is no workaround.

- CSCsv58300

  Symptoms: Classification is not done correctly. It is matching the IPSec header instead of matching parameters in the original header despite “qos pre-classify” configuration.

  Conditions: It has been observed in a Dynamic Multipoint VPN (DMVPN) spoke, GRE tunnel with IPSec protection configured with **qos-preclassify** and applying service policy to the physical interface.

  Workaround: Classify traffic in ingress service-policy marking the traffic. Classify traffic in the egress with the mark inserted in ingress policy.

- CSCsv59334

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

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

  For example:

  router eigrp 1
  network 10.0.0.0
  network 0.0.0.0
  Router# show ip eigrp topo

  EIGRP-IPv4 Topology Table for AS(1)/ID(10.1.1.1)

  Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - reply Status, s - sia Status

  P 10.1.1.1/32, 1 successors, FD is 128256 via Connected, Loopback1 P 10.1.1.0/24, 1 successors, FD is 281600 via Connected, Ethernet1/0 P 10.147.204.64/26, 1 successors, FD is 281600 via Connected, Ethernet0/2 P 10.147.204.0/26, 1 successors, FD is 281600 via Connected, Ethernet0/0

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

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

- CSCsv62225

  Symptoms: Router crashed when PPPoE sessions were cleared and policy was removed.

Conditions: This symptom occurs while removing policy using the **no policy-map name** command.

Workaround: There is no workaround.

- CSCsv62777

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

  ping <cr>
  show clns route <cr>
  ping <cr>
  show clns route 47.0005.8000.0000.0000.0037.0001 <cr>
  show clns <cr> ping clns <cr>

  Conditions: This symptom is observed when an extended ping with CLNS is done and not completed.

  Workaround: Reload the router.

- CSCsv63799

  Symptoms: A router may reload if PfR is enabled and the number of flows exceeds the size of the NetFlow cache. This is a stress condition.

  Conditions: This symptom is observed when PfR is enabled (which also enables NetFlow).

  Workaround: A possible workaround is to configure the following:

  ip flow-cache timeout active 1

- CSCsv64889

  Symptoms: TCP traffic to a router interface is corrupted if the traffic is going through WebVPN with SVC or AnyConnect.

  Conditions: Occurs with AnyConnect or SVC connection and traffic destined to a router interface.

  Workaround: Use IPSec.

  Further Problem Description: The traffic does not fail immediately, but after around 7 seconds.

- CSCsv66215

  Symptoms: Problem with IPv6 when deactivating and then reactivating VPN routing/forwarding (VRF).

  One symptom is a message “Can’t activate address-family ‘ipv6’ ”

  Another aspect is a reference to tableid 10000000 that is reserved and should not apply to VRF.

  Conditions: Occurs when using VRFs. The problem only occurs if IPv6 routing is used and then fully removed. When IPv6 is removed from the system, the IPv6 RIB goes away. One way of reactivating the IPv6 RIB is indirectly to create some VRFs. In that case, it is possible that the tableid 10000000 be allocated to a VRF, in which case the problem occurs.

  Workaround: The path that leads to the problem consists in allocating the IPv6 RIB indirectly via VRFs installation. The problem only occurs at reactivations. There are thus a few ways to workaround:

  - Reboot the router.
  - Configure **ipv6 unicast router** or IPv6 on interfaces before entering VRF configuration.

- CSCsv66513

  Symptoms: When an external interface is shut down, all the applications exiting on that interface do not go to the DEFAULT state.

Conditions: PfR enabled with applications configured to be controlled. More than one application gets controlled on an exit.

Workaround: Set probe interval short.

- CSCsv66827

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

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

  Workaround: There is no workaround.

- CSCsv69784

  Symptoms: A middle buffer leak is observed when using the combination of RIP and multipoint frame relay.

  Conditions: Currently the trigger is unknown.

  Workaround: There is no workaround.

- CSCsv73509

  Symptoms: If “no aaa new-model” is configured, authentication occurs through the local even when TACACS is configured. This happens for EXEC users under the VTY configuration.

  Conditions: The symptom is observed when you configure “no aaa new-model”; configure “login local” under line vty 0 4; and configure “login tacacs” under line vty 0 4.

  Workaround: There is no workaround.

- CSCsv73941

  Symptoms: The **http client cache memory pool 0** command is ignored.

  Conditions: Caching cannot be disabled for the HTTP client.

  Workaround: There is no workaround.

- CSCsv74695

  Symptoms: Saved aux port configurations are lost after a reload on the Cisco 880 series.

  Conditions: Issue can be recreated by changing the aux port configurations under “line aux 0” when the combo console/aux port on the 880 series is in the aux port mode, saving the configs to NVRAM, and then reloading the router.

  Workaround: The following configuration changes can be used to work around the issue:

  line aux 0
  modem InOut
  modem autoconfigure discovery

- CSCsv75948

  Cisco IOS Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available and are documented in the workarounds section of the posted advisory.

  This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml

- CSCsv76110

  Symptoms: Attaching service policy of self-zone policy-map failure to the zone-pair.

  Conditions: When L7 Policy-map of service policy-map attached to the L4 Policy-map.

  Workaround: There is no workaround.

- CSCsv77046

  Symptoms: Dynamic Multipoint VPN (DMVPN) spoke to spoke communication is working through hub if hub router has following command configured:

  no ip nhrp cache non-authoritative

  Conditions: In Cisco IOS Release 12.4(22)T, spoke to spoke communication is going through hub if we have NHRP cache non-authoritative disable in hub. However if downgrade version to 12.4(15)XY3 it worked just fine even **ip nhrp cache non-authoritative** is disabled in hub.

  Workaround: Enable **IP Nhrp cache non-authoritative** in hub.

- CSCsv79343

  Symptoms: Tracebacks with following message will be seen after decrypting TCP packet:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level,
  ```

  Conditions: The configurations use IPSec over GRE. Crypto map is applied on the tunnel interface and the packet is first encrypted with IPSec then encapsulated with GRE. Tracebacks happens after the decryption.

  Workaround: Use GRE over IPSec. Apply crypto map on the physical interface to protect GRE traffic. Or use tunnel protection.

- CSCsv86107

  Symptoms: Cisco 2800 router crashes due to signal 10.

  Conditions: Crash happens while transferring calls.

  Workaround: There is no workaround.

- CSCsv86288

  Symptoms: Sending a NETCONF hello reply which contains a “session-id” element triggers an instant crash. The device will report a reload due to a bus error.

  Conditions: This occurs when sending a hello reply which contains a session-id element. A hello without this element, one which only contains NETCONF capabilities, does not cause a crash.

  Workaround: Send a NETCONF hello without a session-id element.

- CSCsv87146

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

  Conditions: A dynamic translation mapping is removed while traffic is running.

  Workaround: Stop traffic when removing dynamic NAT translation.

  Further Problem Description: NAT translation is created while dynamic mapping is being removed. These entries contains pointers to memory that is no longer available. When these entries are freed, router crash due to illegal memory access.

- CSCsv92292

  Symptoms: The following error message is observed when RITE is applied to the interface.

```
011419: Nov 19 17:53:15.422 CST: %SYS-2-BADBUFFER: Attempt to use contiguous buffer as
scattered src, ptr= 83C60298, pool= 83C6010C -Process= "<interrupt level>", ipl= 4,
-Traceback= 0x808DF468 0x80059428 0x8139A9C0 0x8139AEA4 0x80374540 0x8079DD5C
0x803DEB54 0x8040E938 0x8041235C 0x803FAFB0 0x804D0BA8 0x800AEF4C 0x8001A964
0x8001A964 0x800AF008 0x800B6D80
```

Conditions: The error is observed on a Cisco 181x device with c181x-advipservicesk9-mz.124-15.T6 when RITE is configured on the interface.

Workaround: Remove RITE from the interface configuration.

- CSCsv92662

  Symptoms: Router crash observed consistently.

  Conditions: After having configured a series of CNS commands, upon trying to rollback to a clean configuration, the crash is observed.

  Workaround: There is no workaround.

- CSCsv94099

  Symptoms: Traceback may be seen in relay.

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

  Workaround: There is no workaround.

- CSCsv94905

  Symptoms: c2800: crash at xpfGetACLPATNodeFromMessage.

  Conditions: This symptom is observed under normal Cisco IOS operation.

  Workaround: There is no workaround.

- CSCsw14681

  Symptoms/Conditions:

  Step 1: Configure two Co-op KS.

  Step 2: Use a Cisco IOS Release 12.4(23.7)T image.

  Step 3: Either reload or issue the **clear crypto gdoi** command on both routers.

  Step 4: Let election process complete.

  Step 5: Issue the **show crypto gdoi ks replay** command, and the following is displayed:

  ```
  *Dec 17 05:11:52.707: %GDOI-5-COOP_KS_ELECTION: KS entering election mode in group
  GetvpnAdvanced1 (Previous Primary = NONE) *Dec 17 05:12:27.719:
  %GDOI-5-COOP_KS_TRANS_TO_PRI: KS 10.10.1.1 in group GetvpnAdvanced1 transitioned to
  Primary (Previous Primary = NONE) KS1#sh crypto gdoi ks replay Anti-replay Information
  For Group GetvpnAdvanced1: Timebased Replay: Replay Value : 89.01 secs Remaining sync
  time : Timer is not running <------------
  Anti-replay Information For Group GetvpnAdvanced2: Timebased Replay: Replay Value :
  70.36 secs Remaining sync time : Timer is not running <--------------------
  Anti-replay Information For Group GetvpnAdvanced3: Timebased Replay: is not enabled
  ```

  Workaround: There is no workaround.

- CSCsw15188

  Symptoms: Router crashes when enabling the **debug isdn q931** command.

  Conditions: Problem happens when logging debugs from the **debug isdn q931** command to an external syslog server.

  Workaround: Disable the syslog server when doing the debugs.

- CSCsw18988

  Symptoms: Router crashes while configuring the ACL list for webvpn context under "config-webvpn-acl" mode with Nulls string URL.

  Conditions: Router loaded with c7200-adventerprisek9-mz.124-23.8.T facing this problem.

  Workaround: Configure non-empty URL string for ACL list elements.

- CSCsw19335

  Symptoms: Router crashes at "sslvpn_lock_vw_ctx", when simultaneous users tried to access the webvpn context at same time.

  Conditions: Router loaded with c7200-adventerprisek9-mz.124-23.8.T facing this problem.

  Workaround: There is no workaround.

- CSCsw22791

  Symptoms: The router may crash if gdoi configurations are removed and the **show crypto gdoi** CLI are executed concurrently (i.e.: running on different tty sessions).

  Conditions: Removing the configurations and executing the show command have to be run concurrently.

  Workaround: Avoid removing the configuration and executing the **show crypto gdoi** CLI concurrently.

- CSCsw22906

  Code missing when committing CSCsr37296.

- CSCsw23397

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

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

  Workaround: There is no workaround.

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

- CSCsw23664

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

  Conditions: Occurs on routers running Cisco IOS Release 12.4(15)T and above.

  This issue is resolved in the following releases:

  - 12.4(22)T1
  - 12.4(20)T2
  - 12.4(15)T9

  Workaround: There is no workaround.

- CSCsw24542

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

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

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

Workaround: There is no workaround.

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

- CSCsw24611

  Symptoms: A router configured with BGP and VPN import may crash.

  Conditions: This is a hard to hit race condition. BGP imports a path from VRF-A to VRF-B. The following steps have to take place in exactly this order for the crash to occur:

  1. The next-hop for the path has to become unreachable.

  2. BGP has to re-evaluate the bestpath on the net in VRF-A and result in no-bestpath on the net (because there is no alternative path available).

  3. RIB installation has to process the importing BGP net under VRF-B.

  Step 3 will result in the crash. If, before step 3, the next-hop re-evaluation manages to process the net in VRF-B then it will clear the bestpath and there will be no crash. If, before Step 3, the import code gets a chance to process the net it will clean-up the imported path from VRF-B and then there will be no crash.

  Workaround: There is no workaround.

- CSCsw29842

  Symptoms: Router forced reload/crashed @resource_owner_set_user_context while adding and removing MTU in ATM main and subinterface.

  Conditions: The “no mtu” command on the ATM subinterface modifies the min MTU size to zero. Only if the MTU size is zero will it happen.

  Workaround: Set the MTU size of the subinterface with the default value or the value of the main interface mtu instead of “no mtu” command.

  Further Problem Description: The “no mtu” command on the ATM subinterface modifies the MTU size to zero. It should inherit the default value or the value from the main interface if the main interface has MTU value set. It is not affecting any functionality of MTU.

- CSCsw31019

  Symptoms: A Cisco router crashes.

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

  Workaround: There is no workaround.

- CSCsw31363

  Symptoms: “unknown SFP” error message displayed.

  Conditions: Occurs when inserting Cisco GLC-ZX-SM-RGC SFP (1000-ZX base SFP).

  Workaround: There is no workaround.

- CSCsw35638

  Symptoms: When a Cisco router is the Merge Point (MP) for a protected TE tunnel, and FRR is triggered, two things happen:

  - The primary LSP goes down, and traffic is lost on the protected tunnel.
  - Any PLR that is downstream of the failure will lose its backup.

  Conditions: When a competitor's router is a point of local repair (PLR) and a Cisco router is a merge point, then when FRR is triggered, the Cisco router drops the backup tunnel (in some cases immediately and in other cases after 3 minutes). This causes the primary tunnel that is protected by this backup to go down. The issue has been identified as related to the fact that session attribute flags (link/node protection desired) are being cleared by the competitor PLR when the Path is sent over the backup tunnel.

  Workaround: There is no workaround.

- CSCsw36750

  Symptoms: Call will be disconnected with 2 ipipgw's

  Conditions: In SS-DO case when initial renegotiation Re-INVITE received with only change in media direction then CUBE will not send OLC ACK

  Workaround: There is no workaround.

- CSCsw39039

  Symptoms: A fax relay call may fail.

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

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

- CSCsw42244

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

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

  Workaround: There is no workaround.

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

- CSCsw43948

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

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

  ```
  ip cef
  !
  bridge irb
  !
  interface GigabitEthernet0/1
   no ip address
   no sh
  !
  !
  interface GigabitEthernet0/1.100
  ```

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

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

- CSCsw44230

  Symptoms: High CPU observes with SIP call through NAT. NAT entry timeout timer causes slow entry deletion.

  Conditions: When high volume of SIP calls go through the NAT box.

  Workaround: Fine-tune UDP timeout value.

- CSCsw44760

  Symptoms: icmp-jitter timeout value is lost upon system reload.

  Conditions: The issue occurs upon reload if timeout is less than the default threshold value of 5000 or threshold value not equal to zero.

  Workaround: Set threshold equal to zero or increase the timeout greater or equal to 5000.

- CSCsw45320

  Symptoms: Router crashes after it has shown many tracebacks:

```
%SYS-2-BADSHARE: Bad refcount in retparticle, ptr=xyz, count=0, -Traceback= ...
%SYS-2-BADSHARE: Bad refcount in retparticle, ptr=xyz, count=0, -Traceback= ...
%SYS-2-BADSHARE: Bad refcount in retparticle, ptr=xyz, count=0, -Traceback= ...
```

  Conditions: Router is terminating SSLVPN client sessions.

  Workaround: There is no workaround.

- CSCsw47076

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsw47543

  Symptoms: A router may loses all its free memory and crash.

  Conditions: The symptom is observed when the voice mail system sends a notification to the gateway regarding the availability of any voice messages. The memory leaks occurs in CDAPI_RawS.

  Workaround: Use the **signalling forward none** command under the global configuration “voice service voip”.

- CSCsw49170

  Symptoms: VG20X with SCCP controlled FXS ports have switchover to CME-SRST and then switchback to Cisco Unified CallManager (CCM), and then one-way audio in calls is experienced.

Conditions:

- VG20X running 12.4(22)T
- CME-SRST running 12.4(15)T7
- CallManager running 7.0

The VG20X global configuration has the UCM set for version 7.0, as follows:

sccp ccm <*call-manager-ip-address*>**id** <*identifier*> **version 7.0**

The VG20X global configuration has the CME-SRST set for version 4.1, as follows:

sccp ccm <*cme-srst-ip-address*> **id** <*identifier*> **version 4.1**

Workaround: Enter the following commands:

```
no sccp
sccp
```

- CSCsw49297

  Symptoms: Packet drops and/or delays are observed when sending traffic over a multilink bundle interface.

  Conditions: This symptom may occur during periods of bursty traffic.

  Workaround: Increase the amount of data that a multilink will queue to a member link at any given time using the interface configuration command **ppp multilink queue depth qos** (default = 2). This command may be configured on the serial interfaces or, if the interface is a multilink group member, it may be configured on the multilink interface. For example:

  interface Multilink1 ppp multilink queue depth qos 3

- CSCsw49468

  Symptoms: max-pool CLI does not show up under voice register pool when configured as maximum value

  Workaround: There is no workaround. User can do “show run all” to see the configured value.

- CSCsw50918

  Symptoms: Router is getting crashed at sslvpn_lock_vw_ctx, when simultaneous users tried to access the webvpn context at same time.

  Conditions: Router loaded with c7200-adventerprisek9-mz.124-23.11.T facing this problem.

  Workaround: There is no workaround.

- CSCsw51214

  Symptoms: An Secure Real-Time Transfer protocol (SRTP) call may fail through a Cisco Multiservice IP-to-IP Gateway (IPIPGW).

  Conditions: The symptom is observed when a SRTP call is made between two Cisco Unified CallManager (CCM) with an IPIPGW in between.

  Workaround: There is no workaround.

- CSCsw52431

  Symptoms: VG20X (VG204 and VG202) takes long time to register to SRST.

  Conditions: My scenario, I used:

  - CME-SRST running 12.4(15)T7 (CME 4.1)
  - Cisco Unified CallManager running 7.0(2)
  - VG204 running 12.4(22)T

Workaround:

no sccp
sccp

- CSCsw63356

  Symptoms: The following messages may be seen when bringing up a WIC-1DSU-T1-V2:

  ```
  %SERVICE_MODULE-4-WICNOTREADY: (with traceback) and/or
  WARNING - timeslots command not accepted by service-module % Service module
  configuration command failed: LOCK OBTAIN TIMEOUT.
  ```

  Conditions: The symptom is observed with a Cisco 3825 and a 3845 router where WIC-1DSU-T1-V2 or HWIC-1DSU-T1 is present in one or more WIC/HWIC slots and one WIC-1DSU-T1-V2 is in any of the NM slots. In this setup, the problem will be seen on the highest number WIC/HWIC slot where WIC-1DSU-T1-V2 or HWIC-1DSU-T1 is present.

  Workaround: Use WIC-1DSU-T1-V2 in either WIC slots or NM slots (not in both).

  Alternate workaround: Use a Cisco IOS release prior to 12.4(15)T7.

- CSCsw64933

  Symptoms: A VXML gateway may stop providing audio prompts to caller.

  Conditions: When TTS text contains “&” which is escaped as “&”, the XML parser converts it to “&”. VXML interpreter did not escape it when sending the TTS to server. This causes TTS generates a parse error.

  Workaround: Remove the “&” in the VXML script.

- CSCsw65138

  Symptoms: CME router will reboot due to process bus error randomly. For image: Cisco IOS Software, 3800 Software (C3825-SPSERVICESK9-M), Version 12.4(20)T1, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Wed 24-Sep-08 18:40 by prod_rel_team

  Conditions: No particular condition, but from the stack trace info, we can see some sort of ringing event.

  stack trace from initial traceback

  General information:

  Reason: Traceback Platform: Cisco IOS Software, 3800 Version: 12.4(20)T1 Compiled: 24-Sep-08

  Trace:

  Cisco IOS Software, 3800 Software (C3825-SPSERVICESK9-M), Version 12.4(20)T1, RELEASE SOFTWARE (fc3) Technical Support: http:www.cisco.comtechsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Wed 24-Sep-08 18:40 by prod_rel_team Traceback= 0x633E934C 0x62E266B8 0x62E29614 0x620A061C 0x620D51E0 0x620A1394 0x620AC074 0x6206D3AC 0x6206C86C 0x62077774 0x62077934 0x6208B46C 0x62D292E0 0x62D292C4

  Functions:

  0x633E934C : memcpy (+0xec) 0x62E266B8 : cmm_crs_proc_tr_call_ring (+0x364) 0x62E29614 : cmm_notify_trigger (+0x780) 0x620A061C : OB_Setting_Alert (+0xac) 0x620D51E0 : AFW_FSM_Drive (+0x308) 0x620A1394 : OB_FSM_Drive (+0xac) 0x620AC074 : AFW_M_Destination_Action (+0x164) 0x6206D3AC : AFW_Module_Action (+0xe4) 0x6206C86C : AFW_Object_WalkListeners (+0x274) 0x62077774 : AFW_Process_GetCcqEvent (+0x298) 0x62077934 : AFW_Process_GetEvent (+0x160) 0x6208B46C : AFW_Service_Process_Space (+0x128) 0x62D292E0 : r4k_process_dispatch (+0x1c) 0x62D292C4 : r4k_process_dispatch (+0x0)

Diagnostic:

Software failure. The bugs listed below, if any, are likely to be the root cause of the problem, and upgrading to a version in which the bug is integrated will most probably solve the issue. Most likely bugs (of a total of 9 matches): - CSCsi22430 - B-ACD Crashes CME 4.2, R Fixed in versions : 12.4(11)XW - CSCsj98457 - CMM: Add traceability, R Fixed in versions : 12.4(11)XW4 - CSCsj29857 - Transfer to ICD failed after conference AA, R Fixed in versions : 12.4(11)XW2 - CSCsj49982 - CMM: After connected to AA, xfer to sccp and failed to xfer to ICD, R Fixed in versions : 12.4(11)XW3 - CSCsk89685 - call from SIP trunk to route point failed to transfer to agent or dn, R Fixed in versions : 12.4(19.8)PI8 12.4(15)XZ 12.4(22.3)PI10b 12.4(21.14.9)PIC1 - CSCsq85500 - Add CSTA SingleStepTransfer support, R Fixed in versions : - CSCsg77464 - CMM: minor code cleanup, R Fixed in versions : - CSCse59608 - $$CRS:Incorrect processing INVITE w Replace, R Fixed in versions : - CSCsf11430 - CMM: dangling GCID when PRI-UCCX-SCCP-CTCA-PRI, V Fixed in versions :

Google DDTS link:

Perform unfiltered manual queries: Continue from here.

Rsym output:

-Traceback= 0x633E934C[memcpy+0xec] 0x62E266B8[cmm_crs_proc_tr_call_ring+0x364] 0x62E29614[cmm_notify_trigger+0x780] 0x620A061C[OB_Setting_Alert+0xac] 0x620D51E0[AFW_FSM_Drive+0x308] 0x620A1394[OB_FSM_Drive+0xac] 0x620AC074[AFW_M_Destination_Action+0x164] 0x6206D3AC[AFW_Module_Action+0xe4] 0x6206C86C[AFW_Object_WalkListeners+0x274] 0x62077774[AFW_Process_GetCcqEvent+0x298] 0x62077934[AFW_Process_GetEvent+0x160] 0x6208B46C[AFW_Service_Process_Space+0x128] 0x62D292E0[r4k_process_dispatch+0x1c] 0x62D292C4[r4k_process_dispatch+0x0]

stack trace from main router crash

General information:

Reason: not found Platform: Cisco IOS Software, 3800 Version: 12.4(20)T1 Compiled: 24-Sep-08

Trace:

Cisco IOS Software, 3800 Software (C3825-SPSERVICESK9-M), Version 12.4(20)T1, RELEASE SOFTWARE (fc3) Technical Support: http:www.cisco.comtechsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Wed 24-Sep-08 18:40 by prod_rel_team Stack trace from system failure: FP: 0x66749230, RA: 0x633E934C FP: 0x66749230, RA: 0x62E266B8 FP: 0x66749270, RA: 0x62E29614 FP: 0x66749320, RA: 0x620A061C FP: 0x66749768, RA: 0x620D51E0 FP: 0x667497A8, RA: 0x620A1394 FP: 0x667497D0, RA: 0x620AC074 FP: 0x66749800, RA: 0x6206D3AC

Functions:

0x633E934C : memcpy (+0xec) 0x62E266B8 : cmm_crs_proc_tr_call_ring (+0x364) 0x62E29614 : cmm_notify_trigger (+0x780) 0x620A061C : OB_Setting_Alert (+0xac) 0x620D51E0 : AFW_FSM_Drive (+0x308) 0x620A1394 : OB_FSM_Drive (+0xac) 0x620AC074 : AFW_M_Destination_Action (+0x164) 0x6206D3AC : AFW_Module_Action (+0xe4)

Diagnostic:

Software failure. The bugs listed below, if any, are likely to be the root cause of the problem, and upgrading to a version in which the bug is integrated will most probably solve the issue. For more background information about router crashes, please check : Router Crashes Troubleshooting

Most likely bugs (of a total of 9 matches): - CSCsi22430 - B-ACD Crashes CME 4.2, R Fixed in versions : 12.4(11)XW - CSCsj98457 - CMM: Add traceability, R Fixed in versions : 12.4(11)XW4 - CSCsj29857 - Transfer to ICD failed after conference AA, R Fixed in versions : 12.4(11)XW2 -

CSCsj49982 - CMM: After connected to AA, xfer to sccp and failed to xfer to ICD, R Fixed in versions : 12.4(11)XW3 - CSCsk89685 - call from SIP trunk to route point failed to transfer to agent or dn, R Fixed in versions : 12.4(19.8)PI8 12.4(15)XZ 12.4(22.3)PI10b 12.4(21.14.9)PIC1 - CSCsq85500 - Add CSTA SingleStepTransfer support, R Fixed in versions : - CSCsg77464 - CMM: minor code cleanup, R Fixed in versions : - CSCse59608 - $$CRS:Incorrect processing INVITE w Replace, R Fixed in versions : - CSCsf11430 - CMM: dangling GCID when PRI-UCCX-SCCP-CTCA-PRI, V Fixed in versions :

Google DDTS link:

Perform unfiltered manual queries: Continue from here.

Rsym output:

FP: 0x66749230[etext(0x634036b4)+0x3345b7c], RA: 0x633E934C[memcpy(0x633e9260)+0xec] FP: 0x66749230[etext(0x634036b4)+0x3345b7c], RA: 0x62E266B8[cmm_crs_proc_tr_call_ring(0x62e26354)+0x364] FP: 0x66749270[etext(0x634036b4)+0x3345bbc], RA: 0x62E29614[cmm_notify_trigger(0x62e28e94)+0x780] FP: 0x66749320[etext(0x634036b4)+0x3345c6c], RA: 0x620A061C[OB_Setting_Alert(0x620a0570)+0xac] FP: 0x66749768[etext(0x634036b4)+0x33460b4], RA: 0x620D51E0[AFW_FSM_Drive(0x620d4ed8)+0x308] FP: 0x667497A8[etext(0x634036b4)+0x33460f4], RA: 0x620A1394[OB_FSM_Drive(0x620a12e8)+0xac] FP: 0x667497D0[etext(0x634036b4)+0x334611c], RA: 0x620AC074[AFW_M_Destination_Action(0x620abf10)+0x164] FP: 0x66749800[etext(0x634036b4)+0x334614c], RA: 0x6206D3AC[AFW_Module_Action(0x6206d2c8)+0xe4]

Workaround: There is no workaround.

Further Problem Description: Previous bug id CSCsr06874 fix applied.

- CSCsw66082

  Symptoms: A router crash may be seen at ip_mcast_address_lookup when issuing the **show ip igmp ssm-mapping** *multicast group* command on an SSM-mapping enabled router which makes use of DNS lookup for source list.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(23.10)T.

  Workaround: There is no workaround.

- CSCsw67608

  Symptoms: No symptoms; needed for CSCso89298.

  Conditions: This is observed in Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsw70566

  Symptoms: User is experiencing port block when using STCAPP. Behavior is that when going offhook, no dialtone can be heard. Only performing a shut/no shut on the voice port can bring it back to IDLE and get the dialtone.

  Conditions: Customer is using CUCM and VG224 gateway to connect to analog phones. Skinny is the control protocol.

  Workaround: There is no workaround.

Root Cause Analysis: Before PI9, the VPM layer will never send the disconnect confirmation and the setup_ind at the same time (or within 4 milliseconds). But after PI9, a ddts fix CSCsq97697 changed the behavior. In the case when the user goes onhook. Then, immediately after the hookflash duration is passed, he offhook the phone. Before PI9, this behavior will cause the new call's setup be postponed until the next time the user goes onhook. But now, the setup_ind of the new call will be immediately sent right after the previous call's disconnect confirmation. So, when messages traversed to VTSP layer, because of the nature of the DSMP dsp process, the disconnect_done event has more chance to come later than the new call's setup_ind.

In STCAPP, our design is based on the behavior of the time when it was developed (PI2). So we do not handle that sequence. But now, since this is the behavior, we will have to handle that case when disconnect_done comes after the new call's setup_ind.

Fix and Unit Test: The fix is to enhance the disconnect_done handler to make it more robust and more fault tolerant to accommodate this situation.

Unit test is done and the results are passed.

- CSCsw71188

  Symptoms: A Cisco 7200 series router may lose connectivity to the SDH link.

  Conditions: The symptom is observed under the following conditions:

  1. The Cisco 12416 router receives a PAIS Alarm from the Optical Network.

  2. The interfaces go down and up and the ALARM is cleared from the Cisco 12416 router side.

  3. The Cisco 7200 series router loses connectivity.

  4. The Cisco 12416 router interface POS is still UP, but the ping fails.

  5. After interface is shutdown and re-enabled, it is in serial UP but protocol DOWN from the Cisco 12416 router side.

  6. The link is recovered when the fiber is disconnected and reconnected from the Cisco 7200 series router side.

  Workaround: Disconnect and re-connect the fibers from the Cisco 7200 series router side.

- CSCsw72677

  Symptoms: Router crashes with "no bba-group pppoe".

  Conditions: Happens after unconfiguring "bba-group".

  Workaround: There is no workaround.

- CSCsw74836

  Symptoms: Enabling the **auto qos voip** command under an ATM PVC displays an error.

  Conditions: This symptom is observed with a Cisco 7200 router that is loaded with Cisco IOS Release 12.4(23.12)T.

  Workaround: There is no workaround.

- CSCsw76130

  Symptoms: A crash occurs because of a watchdog timer (CPU HOG).

  Conditions: This symptom is observed when "cns config initial" is used to download a large config (~ 20000 bytes) when "cns config notify diff" is also on.

  Workaround: Add "cns config notify diff" to the config after you have applied the initial config to the device.

- CSCsw78939

  Symptoms: No new sessions can come up using VPDN after a few days.

  Conditions: The root cause is that we leak and run out of SSM switch IDs.

  Workaround: There is no workaround.

- CSCsw79696

  Symptoms: Call over the FXO loop-start cannot be established since gateway's dsp detects reverse-battery signal.

  Conditions: The far-end is able to generate reverse-battery signal when called side is ringing. Plus user configure "supervisory disconnect" to either anytone or dualtone.

  Workaround: There is no workaround.

- CSCsw92379

  Symptoms: Many "IP ARP: Sticky ARP entry invalidated" syslog messages appear, and the RP reloads unexpectedly.

  Conditions: This symptom is observed when a linecard is swapped while thousands of DHCP snooping bindings are present and the **ip sticky-arp** command is configured.

  Workaround: Configure the **no ip sticky-arp** command.

- CSCsw93682

  Symptoms: KS database gets messed up.

  Conditions: Clearing GM database from KS and re-registering GMs with different criteria.

  Workaround: There is no workaround.

- CSCsw95531

  Symptoms: If hook flash occurs during a call that is not connected, interaction between gateway and CallManager will cause large number of zero duration call detail records to be written.

  Conditions: Occurs on VG224 running SCCP STCAPP and with CallManager 4.2.

  Workaround: There is no workaround.

- CSCsw97665

  Symptoms: All www sites are allowed even though local block policy is configured and the allow mode is set to off.

  Conditions: N/A.

  Workaround: There is no workaround.

- CSCsx07114

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsx06457

  Symptoms: A router configured with BGP may generate IPRT-3-NDB_STATE_ERROR log messages. An additional symptom when **bgp suppress-inactive** is configured is that the router CPU usage may get close to 100%.

Conditions: When both BGP and an IGP are advertising the same prefix, the error condition may occur. When in addition **bgp suppress-inactive** is configured high CPU usage by BGP may be seen.

Workaround: Removing the **bgp suppress-inactive** configuration should eliminate the high CPU problem. Removing either the BGP or IGP conflicting routes from the system should clear both symptoms.

- CSCsx11776

  Symptoms: Executing the command “show ip bgp version recent 1” or “show ip bgp version 1” from EXEC mode may cause the Cisco IOS device to crash.

  Conditions: This is seen in affected images that have support for BGP.

  Workaround: Use AAA command authorization to prevent the use of these commands.

  Further Information: A note regarding BGP Looking Glasses for IPv4/IPv6, Traceroute & BGP Route Servers:

  Per http://www.bgp4.as/looking-glasses, BGP Looking Glass servers are computers on the Internet running one of a variety of publicly available Looking Glass software implementations. A Looking Glass server (or LG server) is accessed remotely for the purpose of viewing routing info. Essentially, the server acts as a limited, read-only portal to routers of whatever organization is running the lg server. Typically, publicly accessible looking glass servers are run by ISPs or NOCs.

  Public Looking Glass servers running an affected version of Cisco IOS are specially susceptible to this bug because they provide unauthenticated public access to Cisco IOS devices. Because of this, operators of BGP Looking Glass servers are encouraged to use AAA to prevent execution of the commands mentioned above that are known to crash Cisco IOS software.

- CSCsx15038

  Symptoms: NVgen issue with violate-action commands under policy-map class.

  Conditions: When we configure “violate-action” commands with police cir and exceed under policy-map class, it is not reflecting under show run output. The issue is seen in 124-23.15.T, 124-23.15.T1 onwards. Issue is not seen in 124-23.13.T1. But when we configure violate action individually under policy-map class, it is reflected in show run output.

  Workaround: Do not configure as a whole with policy cir and exceed command. Configure as individual commands.

- CSCsx15370

  Symptoms: EIGRP commands disappearing from interface configuration.

  Conditions: Observed on Cisco routers running Cisco IOS Release 12.4T. EIGRP configuration is removed from the interface following an interface flap.

  Workaround: There are no workarounds.

- CSCsx18860

  Symptoms: Traffic does not pass.

  Conditions: VAM2+ originating traffic, process switching.

  Workaround: There is no workaround.

- CSCsx19577

  Symptoms: Router is crashing while booting with c3270-adventerprisek9-mz.124-22.T1.fc2.

  Conditions: Router should boot properly without any errors.

  Workaround: There is no workaround.

- CSCsx20656

  Symptoms: Trace back after enabling “auto qos voip trust” under fr mode.

  Conditions: This issue is seen with a Cisco 7200 router that is loaded with Cisco IOS Release 12.4(23.15)T2.

  Workaround: There is no workaround.

- CSCsx21482

  Symptoms: “write” or “copy running-config startup-config” or “show run” command executed from the console results in a device reload.

  Conditions: A large number of interfaces (200+) have been configured for RIPv6 and are active. Interfaces which are down will not contribute to the problem.

  Workaround: There is no workaround.

  Further Problem Description: The problem may not always arise. It may happen when the device is busy generating RIPng updates on a large number of interfaces and a command referred to above is entered at the console.

- CSCsx28297

  Symptoms: While the **atm pvp** command is applied under the ATM interface, a router reloads.

  Conditions: This symptom is observed while the **atm pvp** command is applied under the ATM interface.

  Workaround: There is no workaround.

- CSCsx45892

  CSCsw52658 improper code commit resulted in 22T1 build break.

  The current ddts was opened to fix that. The diffs indicate the changes that were needed to fix it.

- CSCsx46297

  Symptoms: EZVPN across DVTI is broken after rekey.

  Conditions: Happens only across DVTI. Is not seen with static interfaces.

  Workaround: There is no workaround.

- CSCsx48272

  Symptoms: A Cisco IOS router that is acting as an EasyVPN client may fail to build the IPSec tunnel and hang in the IPSEC_ACTIVE state as shown in the **show crypto ipsec client ezvpn** command output.

  Conditions: It is s not clear now what condition triggers this failure.

  Workaround: There is no workaround.

- CSCsx48738

  Symptoms: After SVTI tunnels shut and service policy is immediately removed, if attempt to re-add service policy or reconfigure tunnel, the Cisco 7200p crashes.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(20)T2 and 12.4-23.15.T.

  Workaround: Shut down all the tunnels (make sure that queueing gets deactivated) and then remove the service policy.

- CSCsx49555

  Symptoms: Crash at OCE functions after disabling NetFlow by “no ip flow ingress”.

Conditions: Occurs when both crypto and NetFlow configs are applied.

Workaround: Do not run crypto along with NetFlow.

- CSCsx51674

  Symptoms: Agent Entry is not seen:

  Conditions: Roaming interface is configured with CCOA configuration. But the mobile router will not see that interface as usable. Seen only in Cisco IOS Release 12.4(22)T.

  Workaround: Shut and unshut the interface, and the interface will be usable.

- CSCsx57925

  Symptoms: A Cisco IOS Release 12.4(20)T2 image crashes a Cisco 2811 ISR.

  Conditions: This symptom is observed when NAT is configured.

  Workaround: There is no workaround.

- CSCsx59039

  Symptoms: Router crashes at SCCP SPI functions to handle events from STCAPP.

  Conditions: This is a corner case that occurs rarely. Only if STCAPP unregisters its SCCP device (forced by a DSP problem in this case) while the corresponding voice-port is still active (having some internal event in the SCCP SPI queue to be processed after the unregistration), the crash can occur.

  Workaround: There is no workaround.

- CSCsx73867

  Symptoms: A router that is running Cisco IOS Release 12.4(22)T and that is configured for L2L tunnels may intercept pass-thru UDP 4500 packets that are destined to internal client.

  ```
  %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
  destaddr=x.x.x.x, prot=50, spi=0xDD8DEB2(232316594), srcaddr=y.y.y.y.
  ```
  Is logged on the at-fault router.

  Conditions: The router that is running Cisco IOS Release 12.4(22)T is configured for IPsec. Internal IPsec client being NATed on router using nat-t.

  Workaround: There is no workaround.

- CSCsx74657

  Symptoms: Multiple issues are seen on multicast NAT. NAT is adding the number of dynamic entry statistics for every new multicast packet, even though there is already an existing NAT flow entry. This causes the number of dynamic entries to be inconsistent with the output from the **show ip nat trans** command. Also, dynamic NAT entries cannot be deleted with the **clear ip nat trans *** command. Finally, every fragmented multicast packet creates a separate NAT entry.

  Conditions: This symptom is observed when the **ip pim sparse-dense-mode** command is configured on the interfaces with NAT overload.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(22)T

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(22)T. All the caveats listed in this section are resolved in Cisco IOS Release 12.4(22)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Miscellaneous

- CSCef11195

  Symptoms: A Cisco router in which MIPS microprocessors are installed may reload unexpectedly.

  Conditions: This symptom is observed when the router either runs low on memory or attempts to allocate a large amount of memory.

  Workaround: There is no workaround.

- CSCeg49153

  Symptoms: It may take a long time for the IPSec router to detect that the CA server is down while trying to reach it for CRL retrieval.

  Conditions: The symptom is observed on a LAN-to-LAN IPSec tunnel between two routers, where one router is configured for CRL checking.

  Workaround: The situation may be slightly improved by lowering the "tcp synwait" value, for example: ip tcp synwait-time 5

- CSCek58338

  Symptoms: A router may crash because of memory corruption in the chunk memory.

  Conditions: This symptom is observed on a Cisco 7600 series when both the Embedded Resource Manager (ERM) and Bidirectional Forwarding Detection (BFD) are configured. The symptom is platform-independent.

  Workaround: Disable BFD.

- CSCek63963

  Symptoms: Router crashes with a traceback decode showing a divide by 0 error.

  Conditions: Occurs when a rate-based event is configured for a counter that has a value of 0, such as the following scenario:

  1. The customer must be using a Cisco IOS Embedded Event Manager (EEM) rate-based Interface Event Detector (either applet or Tcl script). Rate-based means use of the "rate" keyword in the event specification statement.

  2. The rate calculation is attempted after the counters are cleared and before any samples have been taken.

  Workaround: There is no workaround.

- CSCek71050

  Symptoms: Compared to other Cisco IOS software releases, unusually high CPU usage may occur in the BGP router process on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

  Conditions: This symptom is observed when BGP is learning routes from the RIB, even if redistribution is not directly configured under BGP. (Redistribution from other routing protocols to BGP can exacerbate the CPU usage.)

  Workaround: There is no workaround.

- CSCek72156

  Symptoms: Router might crash while performing nonvolatile generation (NVGEN) with compiled standard ACLs.

  Conditions: Occurs only with compiled standard ACLs. Does not occur without compiled ACLs.

  Workaround: There is no workaround.

- CSCek74114

  Symptoms: ASL Rollback was not able to remove ASL configuration **configuration mode exclusive auto lock-show** from running-config.

  Conditions: failure is seen using ASL Rollback on Cisco 7600.

  Workaround: There is no workaround.

- CSCek75558

  Symptoms: When hardware compression is enabled and an MQC policy is used on an FR PVC, the shaper drops all packets after passing a few.

  Conditions: This symptom is observed with normal traffic flow through the interface.

  Workaround: Replace MQC shaping with FRTS and configure the shape rates in the map class. If LLQ is not required on the PVC, another option is to use software compression instead of hardware compression.

- CSCek76062

  Symptoms: A router crashes because of a block overrun (overwriting the memory block).

  Conditions: This symptom is observed only when templates are exported in the export pak, which is used only in version 9 version of exporting.

  Workaround: Version 5 could be used for exporting.

- CSCek77424

  Symptoms: A Cisco router that is running Cisco IOS Release 12.4(13b) might unexpectedly reload with a bus error.

  Conditions: This symptom happens during normal operation with NAT configured.

  Workaround: There is no workaround.

- CSCsb98906

  Symptoms: A memory leak may occur in the “BGP Router” process.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

  Workaround: Disable the **bgp regexp deterministic** command.

- CSCsc72722

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

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

  Workaround: There is no workaround.

- CSCsg42672

  Symptoms: On a Cisco router running Cisco IOS Release 12.0(32)S4 and configured with BGP and peer-groups, if the Fast Peering Session Deactivation feature is configured in the peer-group, the router automatically configures on the command a route-map with the same name as the peer- group.

  Conditions: Occurs with the following configuration sequence:

```
RR#conf t
Enter configuration commands, one per line.
End with CNTL/Z. RR(config)
```

```
#router bgp 65001 RR(config-router)
#neighbor rrs-client fall-over ? bfd Use BFD to detect failure route-map Route map for
peer route <cr>
RR(config-router)#neighbor rrs-client fall-over
RR#sh ru <snip> router bgp 65001
neighbor rrs-client peer-group neighbor rrs-client remote-as 20959 neighbor rrs-client
update-source Loopback0 neighbor rrs-client fall-over route-map rrs-client <<<<<<<
the route-map does not exist.
```

Workaround: Configure the neighbor individually or use peer-templates.

- CSCsg44748

  Symptoms:

  A Cisco IOS VoIP gateway configured for IPIPGW (CUBE) functionality may crash.

  Conditions:

  A gateway configured for IPIPGW functionality with the command **allow-connections** under **voice service voip** under rare conditions will crash while processing VoIP calls.

  This has been found to occur in some scenarios where a single voip call loops (meaning the call is from the IPIPGW back to the same IPIPGW) through the IPIPGW.

  When this occurs, the following error message may be noticed:

  %SYS-6-STACKLOW: Stack for level Network interfaces running low, 0/9000

  Workaround:

  The workaround is to track down the source of the call looping and correct the problem there.

  The other possible workaround is to introduce another termination point in the RTP packet flow beside the IPIPGW. For example, if interworking with Cisco Unified Communications Manager (Callmanager) a MTP resource may be used to prevent this loop.

- CSCsg45637

  Symptoms: A traceback may be generated when the router accesses the "bgp_vpnv4_lookup_prefix" function.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP VPNv4.

  Workaround: There is no workaround.

- CSCsg92473

  Symptoms: The netflow shortcuts created are cleared before the full capacity of 128k flows (PFC3B) and 256k flows (PFC3BXL) is reached and before the reflexive ACL ageing timers expire. The full capacity is not achieved and active flows may start to get purged.

  Conditions: The symptoms are observed when either the traffic is from 128k or 256k different sources.

  Workaround: There is no workaround.

- CSCsg92618

  Symptoms: Entering the **crypto key zeroize rsa** command causes traceback.

  Conditions: This symptom is observed in router loaded with the Cisco IOS software image.

  Workaround: There is no workaround.

- CSCsg99677

  Symptoms: Crashinfo collection to a disk filesystem will fail and generate the following error message:

File disk#:crashinfo_20070418-172833-UTC open failed (-1): Directory entries are corrupted, please format the disk

Or the crashinfo file will be stored as CRASHI~1.

Conditions: This symptom is observed with normal crashinfo collection to a disk filesystem.

Workaround: Configure the crashinfo collection either to a network filesystem (such as tftp or ftp) or to a local filesystem of type "flash". Configuring to a local filesystem is a preferable option.

Further Problem Description: This happens every time, but there is no major negative impact to operation.

- CSCsh66406

  Symptoms: When you enter the **'maximum route x y'** VRF configuration command or reduce the *limit* argument of the **maximum route** VRF configuration command, stale routes may occur in the BGP VPNv4 table.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the connection with a CE router is configured for another protocol than BGP such as OSPF and when the routes are redistributed into BGP.

  Impacts: May have functional impact.

  Trigger: 'maximum route x y' VRF configuration command.

  Workaround: If OSPF is the other protocol, enter the **'redistribute ospf'** address-family configuration command.

- CSCsi51014

  Symptoms: Disk access causes router to crash.

  Conditions: Occurs after **fsck** execution.

  Workaround: Format disk, which causes the data loss on the affected disk.

- CSCsj36031

  Symptoms: The configuration for "xconnect" may not be accepted.

  Conditions: Problem seen only when the existing "xconnect" configuration is removed from ATM PVC with "encap aal0" and then attached to the same ATM pvc.

  Workaround: Remove the ATM PVC and reconfigure again with aal0 encapsulation and "xconnect".

- CSCsj37877

  Symptoms: Cisco 7200 router crashes when configured as a PE.

  Conditions: Router is configured as provider edge (PE) router in a hub and spoke topology. It is located in the hub. When ping/traceroute commands are issued from a LAN on the hub towards a LAN in the spoke, it causes the Cisco 7200 to crash. Ping/traceroute issued from the other end does not cause a crash, but traffic does not go through the PE.

  Issue was seen with Cisco IOS Release 12.4(15)T. It was not seen with Cisco IOS Release 12.4(11)T.

  Workaround: There is no workaround.

- CSCsj49293

  Symptoms: The interface output rate (214 Mb/s) is greater than the interface line rate (155 Mb/s).

  Conditions: This symptom is observed with a Cisco 7600/7500/7200-NPE400 and below. That is, PA-POS-2OC3/1OC3 (PULL mode).

  Workaround: There is no workaround.

Further Problem Description: From the Ixia, packets are transmitted at 320 Mb/s. On the UUT (Cisco 7600), the outgoing interface (POS-Enhanced Flexwan) shows the output rate as 200 Mb/s. But the interface bandwidth is 155 Mb/s.

- CSCsj56281

  Symptoms: Inherit peer-policy does not work after router reload.

  Workaround: There is no workaround.

- CSCsj64222

  Symptoms: An Cisco router configured with Dynamic Multipoint VPN (DMVPN) may crash when the tunnel interface is shut down and then later **no shut**, or if the tunnel protection configuration is changed.

  Conditions: This occurs with a DMVPN configuration where a spoke router has more than one tunnel interfaces that share the same tunnel source interface.

  Workaround: There is no workaround.

- CSCsj84572

  Symptoms: The **l2 vfi ...** configuration command is rejected by the parser as an ambiguous command.

  Conditions: The symptom is observed when the router is in configuration mode and a command beginning with **l2 vfi** is entered.

  Workaround: There is no workaround.

- CSCsk05653

  Symptoms: The **aaa group server radius** subcommand **ip radius source-interface** will cause the standby to fail to sync.

  ```
  c10k-6(config)#aaa group server radius RSIM c10k-6(config-sg-radius)#ip radius
  source-interface GigabitEthernet6/0/0
  c10k-6#hw-module standby-cpu reset c10k-6# Aug 13 14:49:31.793 PDT:
  %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT) Aug 13
  14:49:31.793 PDT: %C10K_ALARM-6-INFO: ASSERT MAJOR RP A Secondary removed Aug 13
  14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN) Aug
  13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
  (PEER_REDUNDANCY_STATE_CHANGE) Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST:
  Standby processor fault (PEER_NOT_PRESENT) Aug 13 14:49:31.793 PDT:
  %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN) Aug 13 14:49:31.813
  PDT: %REDUNDANCY-3-IPC: cannot open standby port no such port Aug 13 14:49:32.117 PDT:
  %RED-5-REDCHANGE: PRE B now Non-participant(0x1C11 => 0x1421) Aug 13 14:49:32.117 PDT:
  %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
  (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
  Aug 13 14:50:52.617 PDT: %RED-5-REDCHANGE: PRE B now Standby(0x1421 => 0x1411) Aug 13
  14:50:54.113 PDT: %C10K_ALARM-6-INFO: CLEAR MAJOR RP A Secondary removed Aug 13
  14:51:33.822 PDT: -Traceback= 415C75D8 4019FB1C 40694770 4069475C Aug 13 14:51:33.822
  PDT: CONFIG SYNC: Images are same and incompatible
  Aug 13 14:51:33.822 PDT: %ISSU-3-INCOMPATIBLE_PEER_UID: Image running on peer uid (2)
  is the same -Traceback= 415CCC2C 415C75FC 4019FB1C 40694770 4069475C Aug 13
  14:51:33.822 PDT: Config Sync: Bulk-sync failure due to Servicing Incompatibility.
  Please check full list of mismatched commands via: show issu config-sync failures mcl
  Aug 13 14:51:33.822 PDT: Config Sync: Starting lines from MCL file: aaa group server
  radius RSIM ! <submode> "sg-radius" - ip radius source-interface GigabitEthernet6/0/0
  ```

  Conditions: This symptom is observed if the **aaa group server radius** subcommand **ip radius source-interface** CLI is configured on a box with dual PREs.

  Workaround: If the customer does not use the **aaa group server radius** subcommand **ip radius source-interface** *interface*, this will not be a problem.

If they use the **aaa group server radius** subcommand **ip radius source-interface** *interface* on a Cisco 10000 router in simplex mode (a single PRE), this will not be a problem.

If they run with dual PREs, then they will need to remove the **aaa group server radius** subcommand **ip radius source- interface** *interface* from the configuration as a workaround.

Removing the **aaa group server radius** subcommand **ip radius source-interface** *interface* from the configuration could cause problems for the customer. The radius server may be expecting the request to come from a specific source address. The router will now use the address of the interface the packet egresses the router from, which may change over time as routes fluctuate.

- CSCsk06777

  Symptoms: Firewall may inspect traffic that is denied by output ACL.

  Conditions: Occurs when firewall and ACL are applied in the same direction on output interface.

  Workaround: There is no workaround.

- CSCsk28361

  Symptoms: 4000 virtual-template (VT) takes high CPU during system load configuration.

  Conditions: Occurs when 4000 VT interfaces are loaded from TFTP to running configuration.

  Workaround: There is no workaround.

- CSCsk39308

  Symptoms: An asynchronous interface cannot successfully be configured as **ip unnumbered** to a loopback interface. Example:

  Conditions: Occurs with the following configuration:

  ```
  Router(config-if)#interface Group-Async1
  Router(config-if)#ip unnumbered Loopback0
  ```
  Point-to-point (non-multi-access) interfaces only

  Workaround: There is no workaround.

- CSCsk39806

  Symptoms: The command **show bgp all dampening parameters** does not show the VPNv6 unicast address-family. Also, the VPNv6 address family may not be seen in the running configuration.

  Conditions: The symptom is observed when using Cisco IOS Release 12.4(20)T and when using the command **show bgp all dampening parameters**.

  Workaround: There is no workaround.

  Further Problem Description: The output of **show bgp vpnv6 unicast all dampening parameters** works properly. The impact of this issue is primarily display/UI.

- CSCsk42373

  Symptoms: A memory leak may be seen when configuring commands.

  Conditions: The symptom is observed when configuring or unconfiguring MLD snooping commands, but affects all configuration commands.

  Workaround: There is no workaround.

  Further Problem Description: A configuration change tracking ID is invoked when a command is applied. While updating the tracking ID, a new octet string is allocated which causes the memory leak. A leak of 48 bytes per configuration command is seen. This issue affects all platforms.

- CSCsk44568

Symptoms: Counters on input interface and receivers interface are not in sync when rate-limit is applied on input interface.

Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(16.14)T4 with rate-limit configured on input side.

Workaround: There is no workaround.

- CSCsk64158

  Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml.

- CSCsk65460

  Symptoms: Multicast fast switching fails on the decapsulating provider edge (PE) router when encryption is configured.

  Conditions: This happens on a Cisco 7200 router with Cisco IOS Release 12.4(17.4)T1.

  Workaround: There is no workaround.

- CSCsk76053

  Symptoms: When using route-map to redirect the traffic from one physical interface to be rerouted to the loopback interface, the traffic is not redirected.

  Conditions: Occurs when router is configured for "EZvpn client on stick" 1interface inside/outside, loop being the inside.

  Workaround: Configure interface vlan1.

- CSCsl04835

  Symptoms: A route introduced by Conditional Route Injection is not removed from the iBGP peer upon withdrawal.

  Conditions: Consider this situation: Router B is a BGP router that has two eBGP peers, Router A and Router C. In a situation where RTR_A advertises a prefix and RTR_B injects a more specific prefix of it, the symptom is observed in two ways: 1. If RTR_A withdraws the advertised prefix, the more specific prefix is removed on RTR_B, but this withdrawal is not sent to RTR_A and RTR_C. 2. If the conditional route injection configuration is removed on RTR_B, the more specific prefix is removed on RTR_B, but this withdrawal is not sent to RTR_A and RTR_C.

  Workaround: There is no workaround.

- CSCsl13043

  Symptoms: Hub in VPN routing/forwarding (VRF) drops ingress multicast when Cisco Express Forwarding (CEF) is enabled on Dynamic Multipoint VPN (DMVPN) tunnel.

  Conditions: This happens on a Cisco 7200 router running Cisco IOS Release 12.4(17.9)T.

  Workaround: There is no workaround.

- CSCsl44498

  Symptoms: Serial interface (CT1) goes down when attaching a policy with traffic and a class map that has an extended ACL.

Conditions: Occurred on a Cisco 7200 Router with extended ACL with traffic.

Workaround: There is no workaround.

- CSCsl49628

  Symptoms: When a VPN routing/forwarding (VRF) is deleted through the CLI, the VRF deletion never completes on the standby RP, and the VRF cannot be reconfigured at a later time.

  Conditions: This symptom is observed when BGP is enabled on the router.

  Workaround: There is no workaround.

- CSCsl50271

  Symptoms: An Open Shortest Path First (OSPF) enhancement, to avoid a suspend when link state update packets are sent, may result in a router crash.

  Conditions: The symptoms are observed in a scenario with 3k tunnels. Both unconfiguring the loopback interface and deleting the loopback interface trigger the same code path that may lead to OSPF suspension.

  Workaround: There is no workaround

  Further Problem Description: The problem actually exists in all branches. However, this is a timing issue.

- CSCsl51353

  Symptoms: The packets are getting dropped on the ATM subinterface

  Conditions: Occurs when shaping is configured in the policy-map. Enable cef on the router, apply service-policy on the ATM interface of the router and send traffic. Now check for the packets count on the router. Packets will be getting dropped.

  Workaround: There is no workaround.

  Further Problem Description:

  This issue manifests packet drops even in absence of congestion when a service policy configured with any shaping feature is attached to an ATM interface

- CSCsl57075

  Symptoms: Router is configured for Dynamic Multipoint VPN (DMVPN) phase II, spoke-to-spoke communication. Packets are dropped for a particular spoke.

  Conditions: Occurs because corresponding Next Hop Resolution Protocol (NHRP) is not complete.

  Workaround: There is no workaround.

- CSCsl64470

  Symptoms: The IOS device may reload when **cns config notify** is configured.

  Conditions: Occurs only when **cns config notify** is configured.

  Workaround: Do not use this command.

- CSCsl92316

  Symptoms: Router may experience mwheel CPUHOG condition.

  Conditions: This condition is observed on Cisco router while clearing all L2TP sessions when there are more than 2500 sessions with multicast traffic flowing on the sessions.

  Workaround: There is no workaround.

- CSCsl99275

Symptoms: High CPU can be seen on Cisco AS5400XM after given uptime.

Conditions: Occurs after 2-3 weeks uptime. CPU usage increases because of "Background Loade" process.

Workaround: Reload the access server.

- CSCsm10603

  Symptoms: L2TP sessions flap both when idle and when traffic is being passed.

  Condition: Occurs on an internal version of Cisco IOS Release 12.4T only on the Cisco 1760 platform and while the voluntary tunneling feature is invoked.

  Workaround: There is no workaround.

- CSCsm13968

  Symptoms: A router crashes when a service policy with FPM is configured, removed, and reconfigured on an interface.

  Conditions: This symptom is seen only when the service policy is configured, then removed, and reconfigured on the same or a different interface.

  Workaround: There is no workaround.

- CSCsm30584

  Symptoms: A CWPA2 card and device may crash after attaching and removing the service policy.

  Conditions: The symptom is observed when the VT is configured with a service- policy and the policy is applied to a PVC on the sub-interface. (The output from the **show policy-map int** command shows that both policies are active under V-access.) Then the policy is removed from the VT and the **shutdown** followed by the **no shutdown** commands are executed on the main interface or sub- interface, or the module is reloaded.

  Workaround: There is no workaround.

- CSCsm34002

  Symptoms: CPU utilization goes to 99%. It stays there for few seconds, then reduces to around 50%, then 2%. After few seconds, CPU utilization reaches 99%, and this cycle continues.

  ```
  ROUTER#show proce cpu sorted
  CPU utilization for five seconds: 99%/0%; one minute: 47%; five minutes: 25%
  ```

  Conditions: This symptom is observed when around 2000 PPPOE sessions are initiated.

  Workaround: There is no workaround.

- CSCsm34226

  Symptoms: Router crashed during stress test of 5000-6000 56-byte UDP packets per second.

  Conditions: Occurred on a Cisco 878 router running 12.4(15)T1.

  Workaround: There is no workaround.

- CSCsm47111

  Symptoms: Traceback is seen.

  Conditions: Occurs when certain memory checking is enabled.

  Impact: This is a fairly harmless issue. No impact.

  Workaround: Disable memory checking.

- CSCsm48357

Symptoms: When FlexWAN card configured for Frame Relay over MPLS (FRoMPLS) is subjected to online insertion and removal (OIR), the standby will crash when FRoMPLS is unconfigured.

Conditions: Occurs when FRoMPLS is unconfigured following an OIR

Workaround: There is no workaround.

- CSCsm50309

  Symptoms: Border router crashes due to heartbeat failure while configuring Optimized Edge Routing (OER).

  Conditions: Occurred while configuring OER in a border router. After the **master IP key- chain password** was entered, the master came up and enabled netflow aggregation export v9, the CPU hung, and the device crashed.

  Workaround: There is no workaround.

- CSCsm54614

  Symptoms: A service-policy may not be removed from a frame relay map-class when the FR-DLCI's circuit is reduced to less than the configured bandwidth of the policy-map.

  Conditions: The symptoms are observed under the following conditions: - A policy with an absolute bandwidth is configured and then configured as a service-policy in a Frame Relay map-class. - The FR-DLCI's circuit is reduced to less than the configured bandwidth of the policy map.

  Workaround: Manually remove the service-policy from the map-class.

- CSCsm57494

  Symptoms: BGP update is not sent after reloading opposite router or resetting module. Sometimes a BGP VPNv4 label mismatch also occurs between the routers because BGP update is not received.

  Conditions: - This problem may occur once or twice out of 20 attempts. - This problem is apt to occur when MPLS-TE tunnel is enabled. - This problem may occur when entering either **reload** command, **hw-module module X reset** command or the **clear ip bgp X.X.X.X** command on the opposite router.

  Workaround: There is no workaround.

- CSCsm73592

  Symptoms: A reload may occur when an anything over MPLS (AToM) VC is torn down. Bug triggered initial crash of SIP-400 in slot 4 & ES20 in slot 3. Both cards had to be powered down and reset from the console to recover.

  Conditions: Occurs when AToM VC is setup and torn down later.

  Workaround: There is no workaround.

  Further Problem Description: The crash may occur when an event triggers access to a previously set up AToM VC. For example, the crash may occur when fast reroute (FRR) is configured on the tunnel interface and the primary interface is removed, such as in the following scenario:

  ```
  pseudowire-class ER1_to_HR1_EoMPLS no preferred-path interface Tunnel501331
  disable-fallback ! interface tunnel501331 shutdown ! no interface tunnel501331
  ```

- CSCsm73602

  Symptoms: High CPU load due to VTEMPLATE Backgr process.

  Conditions: Occurs when **ip multicast boundary** command is used on many interfaces (8000 or more).

  Workaround: There is no workaround.

- CSCsm74168

Symptom: Cisco Unified Border Element (CUBE) crashes when operating in SIP to SIP mode. This will happen if CUBE has received REFER on one leg and trying to send INVITE on the other leg as a part of call-transfer..

Conditions: Topology: [CRASH] Org.--(SIP Trk)--CSPS--(SIP Trk)--CUBE1--(SIP Trk)--CUBE2--(H323 Trk)--Term_1 | |(H323 Trk) | Term_2

Call was established b/w Org and Term_1 and the originator attempted to transfer the original call to a second party on the Term_2 side. When this party(Term_2) answered, CUBE1 crashed.

Workaround: There is no workaround.

Further Problem Description:

CUBE1 in detail: X-OR----------CUBE1--------(Term_1)X-EE----- | | | CUBE2 | | -----(Term_2)X-TO----------

X-EE and X-OR operates in SIP-SIP mode.. When it tries to setup new call to Term_2, it tries to get channels, xcaps, callParams info from the peer leg(the Term_1 leg is the peer leg for Term2.) Term_1 call leg passes channels, xcaps, but do not pass callParams details(that contains the operating mode). So the Term_2 leg takes the default and set it's mode as SIP-H323 and executes some of the H323 related function and after that result is undefined and this leads to crash.

- CSCsm75286

  Symptoms: A route-map which is configured with both IPv4 and IPv6 for a BGP peer does not work as expected

  Conditions: Observed after the route-map is modified to delete a sequence.

  Workaround: Apply a fresh route-map.

- CSCsm85249

  Symptoms: Mobile IP (MoIP) tunnel never comes up on a mobile router when roaming to the cellular interface. This is because the HWIC-3G-GSM never receives or accepts the registration reply from the Home Agent.

  Conditions: Occurred on a Cisco 3845 router

  Workaround: There is no workaround.

- CSCsm87721

  Symptoms: Dialer Cisco Express Forwarding (CEF) with IP accounting fails with packet counters returning zero for the member interface.

  Conditions: This happens when **ip accounting output-packets** configured on NAS. The NAS is being checked for **show adjacency detail** which returns 0 packets and 0 bytes for the member interface.

  Workaround: There is no workaround.

- CSCsm87884

  Symptoms: During performance testing, a 20 percent CPU utilization increase is noticed between Cisco IOS Release 12.4(9)T7 and Release 12.4(15)T3. The increase in CPU utilization is seen with 300 byte cos2, cos3 and cos4 traffic only.

  Conditions: The symptom is observed when QoS is configured on the router. It is seen with Cisco IOS Release 12.4(15)T and may also apply to Cisco IOS Release 12.4(11)T.

  Workaround: There is no workaround.

- CSCsm89795

  Symptoms: The router keeps reloading and complaining about unavailability of memory.

Conditions: This symptom is observed if the router is directly connected to a DHCP server or if an attack is made by flooding DHCP replies.

Workaround: There is no workaround.

- CSCso00383

  Symptoms: Multicast VPN scenario may not work due missing Border Gateway Protocol (BGP) multicast distribution tree (MDT) Route Distinguisher (RD) type 2 updates not being sent by provider edge (PE) supporting new style updates (IPv4 MDT address-family)

  Conditions: Issue is seen on Catalyst 6000 series switch running Cisco IOS Release 12.2(33)SXH1.

  Workaround: There is no workaround.

- CSCso07520

  Symptoms: In a high availability/stateful switchover (SSO) environment, when a switchover occurs, an established OSPFv3/BFD peer will flap.

  Conditions: The environment in which this issue can be reproduced is one of an route processor (RP) SSO state along with the configuration of at least one OSPFv3 BFD client. A series of one or more RP/SSO switchovers will cause a BFD peer/link flap.

  Workaround: The only workaround at this point is to not execute or trigger an RP/SSO switchover with any established OSPFv3 BFD peers.

- CSCso12305

  Symptoms: The IPv6 Cisco Express Forwarding (CEF) table may be missing prefixes which are present in the IPv6 RIB.

  Conditions: Occurs when CEF is disabled and re-enabled.

  Workaround: Enter the **clear ipv6 route ***.

- CSCso13102

  Symptoms: Configuring a QoS policy, including Control Plane Protection (CPPr) and Control Plane Policing (CoPP), using ACLs with overlapping ACEs can cause ACEs to be skipped or processed out of order.

  Conditions: When ACLs are used with CPPr, CoPP, or standard QoS policies, ACEs may be skipped when examining traffic that may match more than one ACE. For example, the following ACL is used with a CPPr configuration that is applied to the aggregate control-plane interface.

  ```
  access-list 110 deny icmp host 192.168.100.1 any access-list 110 permit icmp host
  192.168.100.1 any access-list 110 deny icmp any any access-list 110 permit icmp any
  any
  ```

  Sending pings from 192.168.100.1 to 10.255.255.102 results in the following **show access-list** output, and the incoming pings are in fact dropped.

  ```
  Router# show access-list
  Extended IP access list 110 10 deny icmp host 192.168.100.1 any 20 permit icmp host
  192.168.100.1 any (11 matches) 30 deny icmp any any 40 permit icmp any any (5 matches)
  ```

  Workaround: Remove overlapping ACE entries or rework the ACL.

- CSCso15740

  Symptoms: The "set metric" clause in the continue route-map sequence is not setting metric correctly in some particular conditions. This is also applicable in case where the nexthop setting is done via route-map with a continue clause.

Conditions: The symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(32)SY4. This is platform independent. This symptom occurs if the route-map has a continue clause and the match condition does not allow the continue clause to be executed. The following route-map sequence which has to be executed will not execute properly if the metric or nexthop of the prefix are to be modified via the route-map.

Workaround: Avoid using "continue" in a route-map and modifying metric or nexthop via the following route-map sequence.

- CSCso19662

  Symptoms: Tracebacks are seen after unconfiguration when using the **clear ip nat translation *** command.

  Conditions: This traceback occurs with the c7200-js-mz.124-18a.fc2 image.

  Workaround: There is no workaround.

- CSCso21888

  Symptoms: Router may spontaneously reload.

  Conditions: Occurs on routers configured with iSPF computation algorithm in OSPF.

  Workaround: Disable iSPF.

- CSCso28309

  Symptoms: Ping fails from reflector during internal testing.

  Conditions: The goal of the test is to verify the successful termination of PPP/PPPoE over ATM sessions on router's ATM interface using auto sensing. It is performed with auth_pap, process switch, and keepalive disabled. This has a functional impact as the virtual access entry is not getting added to the routing table after doing clear ip route.

  Workaround: There is no workaround.

- CSCso30234

  Symptoms: Encrypted multicast packets are being dropped with VPN Acceleration Module 2+ (SA-VAM2+).

  Conditions: Occurs when multicast packets are being sent out on more than one interface.

  Workaround: There is no workaround.

- CSCso33848

  Symptoms: PPP call may fail with stack group configured.

  Conditions: Failure will happen only when call initiated to stack group member

  Workaround: Initiate PPP call directly to stack group master.

- CSCso37578

  Symptoms: When issuing **media play** command to play media in TCL IVR, it does not play. Script itself is working.

  Conditions: This problem is observed in the following conditions: - Using Cisco 1760 chassis (The problem is not observed on Cisco 2801 chassis) - Using Cisco IOS Release 12.4(15)T. Cisco IOS Release 12.4(11)T or earlier releases do not have this problem) - Using its-CISCO.2.0.1.0.tcl.

  Workaround: Type the **debug voip app kadis_togg** in the router enable mode. The prompt play will start working on Cisco 1700 series router.

- CSCso39597

Symptoms: The redundant RP in a dual-RP router may crash in certain cases when BGP is unconfigured and then an SSO is performed.

Conditions: The symptom is observed on a redundant RP in a dual-RP router that is running Cisco IOS Release 12.2(33)XN with BGP VPNv4 configuration. It is observed when BGP is unconfigured first and then an SSO is performed.

Workaround: Avoid unconfiguring BGP prior to an SSO.

Further Problem Description: The problem is platform independent. After the reset, the redundant RP is able to function normally.

- CSCso39886

  Symptoms: A router crashes when PPPoE sessions are coming up.

  Conditions: This symptom is observed on a Cisco 7301 router when QoS policing is applied to the PPPoE sessions.

  Workaround: There is no workaround.

- CSCso47048

  Symptoms: A router may crash with the following error message:

  ```
  %SYS-2-CHUNKBADFREEMAGIC: Bad free magic number in chunk header, chunk 6DF6E48 data
  6DF7B48 chunk_freemagic EF430000 -Process= "Check heaps", ipl= 0, pid= 5,
  -Traceback= 0x140C170 0x1E878 0x1EA24 0x1B4AC 0x717DB8 chunk_diagnose, code = 2 chunk
  name is PPTP: pptp_swi
  current chunk header = 0x06DF7B38 data check, ptr = 0x06DF7B48
  next chunk header = 0x06DF7B70 data check, ptr = 0x06DF7B80
  previous chunk header = 0x06DF7B00 data check, ptr = 0x06DF7B10
  ```

  Conditions: Issue has been seen on Cisco 7200 router with NPE-G2 configured for L2TP and running Cisco IOS Release 12.4(15)T3 and Cisco IOS Release 12.4(15)T4.

  Workaround: There is no workaround.

- CSCso51637

  Symptoms: Router crashes.

  Conditions: Router may crash in some cases after removing interface Auto-template and unconfiguring auto-mesh with large number of active mesh auto-tunnels. Currently, this crash has only been observed occasionally with internal scale test scripts and has not occurred with manual configuration.

  Workaround: Wait till all auto-tunnels are down after unconfiguring auto-tunnel mesh globally, and before removing interface Auto-template

- CSCso51749

  Symptoms: QoS works fine with unicast packets over a GRE tunnel, but it does not work for multicast over GRE tunnels.

  Conditions:

  1. Apply a simple policing policy on a GRE tunnel. 2. Build an mroute table entry. 3. Send multicast traffic switched over the tunnel. 4. Verify the police functionality.

  Workaround: There is no workaround.

- CSCso52344

  Symptoms: On an RP, the **show ip cef** command displays the nexthop as drop for the 224.0.0.0/4 prefix, but on the linecard the nexthop is displayed as multicast.

  Conditions: This issue occurs when **ip multicast-routing** is not configured and when the command **show ip cef** is issued on the RP and linecard.

Workaround: There is no workaround.

Further Problem Description: This is a cosmetic issue.

- CSCso52598

  Symptoms: The router may crash after the **no interface ethernet** *0/0.1* command is entered.

  Conditions: It could happen on a router with more than 4000 dynamic ARP entries.

  Workaround: Do not execute **no interface ethernet** *0/0.1*.

- CSCso52837

  Symptoms: While executing "copy run disk0:test" the following error is received: %Error parsing filename (No such device)

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

  Workaround: Use a "/", as in "copy run disk0:/test".

- CSCso53496

  Symptoms: When using Group Encrypted Transport VPN (GET VPN) feature, the df-bit override (on IPSec packets) feature is not working. This means that **crypto ipsec df-bit set|clear** commands have no effect, both on a global or per-interface basis.

  Conditions: The bug is only seen when GETVPN is used. Legacy IPSec tunnels are not affected.

  Workaround: There is no workaround.

- CSCso53839

  Symptoms: The router crashes giving bus error when **ip inspect WAAS** is enabled globally and voice traffic is intercepted.

  Conditions: Occurs when **ip inspect** WAAS is enabled globally and a voice call is made.

  Workaround: Disable or remove **ip inspect WAAS**.

- CSCso54167

  Symptoms: BGP peers are stuck with table versions of 0. BGP peers do not announce any routes to neighbors.

  Conditions: Whenever the interfaces flap with online insertion and removal (OIR) multiple times, all of the BGP peers using such interfaces for peering connections encounter this issue.

  Workaround: Delete and reconfigure the neighbor.

- CSCso57886

  Symptoms: A Cisco IOS device may crash with a data bus error exception and stack trace PC = 0xA0000100

  Conditions: Device is running normal production traffic. Presence of malformed punted RP packets in this network caused the issue.

  Workaround: There is no workaround.

- CSCso60063

  Symptoms: Router crashes when the **no password pass** is issued from the console while configuring "dot1x credentials" in configuration mode.

  Conditions: Occurs only when the **no password pass1** command is entered.

  Workaround: There is no workaround.

- CSCso62166

Symptoms: Device crashes while debugging Border Gateway Protocol (BGP) IPv6 unicast updates entering the **clear bgp ipv6 uni *** command.

Conditions: Debugging must be on to see the crash

Workaround: Use the **no debug bgp ipv6 unicast update** command to turn off BGP IPv6 unicast updates debugging.

- CSCso62266

  Symptoms: Router forwards Bridge Protocol Data Unit (BPDU) after disabling spanning-tree. But after reload, it blocks the BPDU.

  Conditions: Occurs when switch-port is configured.

  Workaround: Enable spanning-tree. You may then disable it again if it is not desired.

- CSCso62526

  Symptoms: Standby supervisor reloads after the interface configuration command **no flow-sampler <name>** is used to remove flow sampler map.

  Conditions: Occurs on a Cisco 7606s with two RSP720-3C-GE configured for normal use with sampled NetFlow configured. To cause the issue, a sampler must be explicitly detached.

  Workaround: There is no obvious workaround to the issue. To avoid the issue, avoid detaching the sampled NetFlow.

- CSCso63263

  Symptoms: The RP will start showing IPC-5-WATERMARK: 988 messages pending in xmt for the port messages on the screen. The number of messages will change.

  Conditions: The router has 275,000 i-BGP routes injected into the router. Among these routes, 100,000 are flapped continuously for one to one and half days. They are flapped every 10 sec. The problem needs at least a days worth of time of continuous flapping.

  Workaround: Stop the route flap. Although the messages will keep coming, there is no impact on functionality. And they are bogus since they are originated from wrong count.

- CSCso64104

  Symptoms: A router may crash after applying the configurations related to PA- MC-2T3-EC immediately after the router reloads.

  Conditions: The symptom is observed on Cisco 7200 series and a 7301 router.

  Workaround: Do not configure PA-MC-2T3-EC immediately after the router reloads.

- CSCso64607

  Symptoms: A router may crash when the **no ip vrf** command is issued.

  Conditions: The symptom occurs when VRF was previously configured on a tunnel interface that has subsequently been removed.

  Workaround: Possibly unconfigure **ip vrf** before unconfiguring the tunnel interface.

- CSCso64889

  Symptoms: A router log contains the following error message, and its performance becomes severely degraded:

  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs 4/3),process = DNS Server.

  Conditions: This symptom is observed on a Cisco router that performs many DNS lookups.

  Trigger: This symptom occurs when there are many DNS lookups, but it may also occur otherwise.

Impact: This bug impacts performance.

Workaround: Configure the router in such a way to prevent it from performing many DNS lookups, and do not configure the router as a DNS server for other devices.

Further Problem Description: Note that CSCsg64586 can produce very similar symptoms, even in the absence of a large number of DNS queries.

- CSCso65193

  Symptoms: The memory occupied by the IP SLA Event Processor may gradually increase.

  Conditions: The issue occurs when IP SLA jitter operation is configured on the router without source port specification.

  Workaround: There is no workaround.

  Further Problem Description: With 1000 IP SLAs configured (200 each of following types: path-echo, path-jitter, icmp-echo, udp-jitter and udp-echo, each with a unique destination), the memory allocated for "IP SLAs Event Pr" increases and the level of available processor memory goes down. This issue will have a performance impact.

- CSCso66396

  Symptoms: If the dialing process is interrupted with a Carrier Drop message, it is not possible to attempt a new call for that remote site.

  Conditions: After receiving a Carrier Drop message, the dialer is not cleared. The **show dialer session** command reports status 6 for that call. Traffic directed to the remote site is dropped. The dialer map is still active. All the traffic is still routed to the dialer and dropped.

  Workaround: Clear the dialer session.

  Further Problem Description: This will impact traffic forwarding.

- CSCso66473

  Symptoms: A router may crash when the user moves from one segment to another and attempts to log onto SSG.

  Conditions: The symptom is observed in the following situation: 1. Open a user known to SSG through accounting-start, with an IP address of "IP1." 2. User then logs onto SSG. 3. User moves to another segment which generates another accounting-start for the same mac address but a different IP address, IP2. 4. The SSG then crashes.

  Workaround: There is no workaround.

- CSCso66516

  Symptoms: Memory allocated at function "_fib_table_test_cef_table_route_list" function is leaked.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS 12.2(33.02.19)SBK06 and that is configured for CEF-MTR

  Workaround: There is no workaround.

- CSCso67141

  Symptoms: When a Border Gateway Protocol (BGP) peer is brought down, some of the routes that were learned may not be removed. If around 200,000 routes are advertised from a neighbor and the BGP process on the neighbor is then stopped, all routes will be removed the first time. On the second time, however, around 20,000-80,000 routes may remain.

  Conditions: The symptom occurs when the BGP process on the neighbor (that has advertised 200,000 routes or more) is brought down.

  Workaround: There is no workaround.

- CSCso78897

  Symptoms: A Cisco 870 router will process and forward packets received with a multicast MAC address even though it should not, such as when the interface controller does not own the multicast MAC address.

  Conditions: This was observed on a Cisco 878 Router running Cisco IOS Release 12.4(15)T4.

  Workaround: Make sure the switch connecting to the Cisco 870 does not send packets with multicast MAC addresses that should not be received by the Cisco 870.

- CSCso82469

  Symptoms: If a user tries to create new mail, the OWA displays an improper message (such as the page cannot be displayed or that the page cannot be loaded) and the OWA session hangs. This will cause the rest of the session to be unresponsive to any more connections.

  Conditions: The symptom is observed on a server configured with the OWA feature. The issue only occurs when trying to access OWA.

  Workaround: There is no workaround.

- CSCso82732

  Symptoms: Every hour (at 31 mins past the hour), three to six calls fail. The cause is given as "cause 47" (resource not available) and "cause 16" (cause 16 errors usually follow cause 47 errors).

  Conditions: The symptoms are observed every hour under load conditions when 20 or more T1 channels are turned on. No errors are seen with a load less than 20 channels.

  Workaround: Use Cisco IOS Release 12.4(15)T5. Alternatively, remove the NTP configuration from the GK.

  Further Problem Description: CPU spikes are seen at the time of failures on NTP process. There are no call failures if the NTP configuration is removed.

- CSCso87348

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly.

  Conditions: Occurs when NetFlow is configured on one of the following:

  * Cisco 7600 running Cisco IOS Release 12.2(33)SRC. * Catalyst 6500 running Cisco IOS Release 12.2SXH.

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

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

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

- CSCso87916

  Symptoms: Router may crash when booting with large number of interfaces configured for RIP for IPv6 (RIPng).

  Conditions: Occurs when RIPng is configured on 1000 or more interfaces.

  Workaround: There is no workaround.

- CSCso88429

  Symptoms: CME or CUBE will reject an inbound SIP INVITE if Max-Forwards is greater than 70.

  Conditions: The symptoms are observed when a Max-Forwards header field in SIP INVITE is greater than 70.

  Workaround: There is no workaround.

Further Problem Description: From RFC 3261: 20.22 Max-Forwards

The Max-Forwards header field must be used with any SIP method to limit the number of proxies or gateways that can forward the request to the next downstream server. This can also be useful when the client is attempting to trace a request chain that appears to be failing or looping in mid-chain.

The Max-Forwards value is an integer in the range 0-255 indicating the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request. The recommended initial value is 70.

This header field should be inserted by elements that can not otherwise guarantee loop detection. For example, a B2BUA should insert a Max-Forwards header field.

- CSCso89794

  Symptoms: Spurious accesses are seen when SNMP queries are performed on the router.

  Conditions: This symptom occurs if SNMP queries like "snmpwalk -v2c 7.42.19.43 public .1.3.6.1.4.1.9.3.6.13.1" are performed on the router. Spurious accesses are seen.

  Workaround: There is no workaround.

- CSCso91078

  Symptoms: A Cisco IAD2430 may reload unexpectedly because of a bus error (Sig=10).

  Conditions: The symptom is observed on a Cisco IAD2430.

  Workaround: There is no workaround.

- CSCso91341

  Symptoms: The following operations are legal but are rejected on the grounds that there is insufficient bandwidth: 1. A QoS policy-map is attached as a service-policy to an interface or other valid target; or 2. A previously attached policy-map is modified.

  Conditions: The symptoms are observed when, prior to the error, a policy-map failed to be attached or modified due to insufficient bandwidth to meet the bandwidth guarantees in the policy-map.

  Workaround: Remove all policy-maps from the affected target. Attach a simple policy-map with no bandwidth guarantees (e.g., having only a **shape** command). Remove this service-policy. This should remove all queueing datastructures from the target. Proceed to attach the original policy-map.

- CSCso92175

  Symptoms: The configured value of a queue-limit gets changed and locked at 16000 bytes when random-detect is applied to the policy-map and service policy is attached to the interface.

  Conditions: The symptom is observed when a queue-limit is configured in front of the WRED in the same class of policy-map.

  Workaround: Configure the WRED in front of queue-limit in the same class of policy-map.

- CSCso93065

  Symptoms: Standby RP crashes while receiving dynamic sync from active RP during DHCP relay binding creation.

  Conditions: Occurs when outer is configured as DHCP relay and running IOS images that include the fix for CSCsm86039.

  Workaround: There is no workaround.

- CSCso93867

  Symptoms: Router crashes with bus error exception.

Conditions: This happens when **qos service-policy** is unconfigured or reconfigured on a virtual-template interface.

Workaround: There is no workaround.

- CSCso94507

  Symptoms: A router may crash when attaching a service policy to an IMA group interface.

  Conditions: The symptom is observed when a service policy is applied to the PVC of an IMA group interface.

  Workaround: There is no workaround.

- CSCso95136

  Symptoms: Cisco 181x series router crashes.

  Conditions: Occurs while unconfiguring dialer in band on asynchronous interface.

  Workaround: There is no workaround.

- CSCso97593

  Symptoms: Cisco ASR1000 loses QoS configuration after reload.

  Conditions: Cisco ASR1000 will lose the configuration if flat service policy is configured on Multilink Point-to-Point Protocol (MLPPP) bundles.

  Workaround: This problem is not seen if MLPPP bundles are configured with hierarchical service policy.

- CSCso98430

  Symptoms: A PPPoE session fails to come up.

  Conditions: This symptom is observed on a Cisco router loaded with Cisco IOS Release 12.4T, and when virtual-template is configured.

  Workaround: There is no workaround.

- CSCsq03115

  Symptoms: The PIM configuration may be missing and the following traceback is seen:

  ```
  %SYS-3-MGDTIMER: Running timer, init, timer = 895661C. -Process= "Exec", ipl= 0, pid=
  80, -Traceback= 0x14C0F30 0x31DA638 0x31DA7C8 0x31DA914 0x1E019B4 0x1E35634 0x1E34AD0
  0x15160F8 0x1515234 0x1542208 0x695548
  ```

  Conditions: The symptom is observed symptom is observed after performing an OIR of the PA-T3+ serial port adapter. The symptom occurs twice.

  Workaround: Reconfigure the PIM mode.

- CSCsq04673

  Symptoms: A switch running Cisco IOS Release 12.2(33)SXH1 may show a SIGSEGV error.

  Conditions: The symptom is observed when EEM policies are configured. The issue will take effect when both: a) An EEM policy with event syslog is executed; and b) The system does not have any memory left.

  Workaround: There is no workaround.

  Further Problem Description: The issue is not specific to ION images as IOS images are also impacted. It is not platform specific.

- CSCsq05099

  Symptoms: User can only configure a maximum of 500 SWMTP sessions per profile.

Conditions: This symptom is observed when using SWMTP.

Workaround: Configure multiple SWMTP profiles.

- CSCsq05997

  Symptoms: The following error messages may appear in the log file multiple times:

  ```
  %ARP-3-ARPINT: ARP table accessed at interrupt level 1, -Traceback= 0x61013944
  0x60B61F80 0x60B5A2A4 0x6019DDAC 0x600FA37C 0x600FCC6C Because the message is
  generated frequently, the log file may fill up too soon.
  ```

  Conditions: The symptom is observed because an IOS component is accessing the arp cache table in the interrupt context, which against the design of the IOS module. The error message indicates that the software is in danger of causing the router to crash.

  Workaround: There is no workaround.

- CSCsq06645

  Symptoms: Packets may get dropped when a route map is applied to peergroup members.

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4T. The problem is seen when the combination of peergroup and route map is used.

  Workaround: There is no workaround.

- CSCsq09592

  Symptoms: The router is black-holing traffic that is going to be encrypted. The crypto-counters are not showing an increase.

  Conditions: The symptoms are observed when service-policy is configured on the main interface and crypto map is configured on a subinterface and when IP CEF is enabled.

  Workaround: Redesign the configuration to apply service policy on the subinterface. Disable CEF globally.

  Further Problem Description: Clear text-traffic is effectively received by the router. It triggers the creation of Phase I/Phase II. However, it then appears to be blackholed:

  ```
  interface Ethernet0/0 no ip address service-policy output shape ! interface
  Ethernet0/0.10 encapsulation dot1Q 10 ip address 10.0.0.1 255.255.255.252 crypto map
  mymap
  ```

- CSCsq09836

  Symptoms: 1. For some 3660 platform images, the **connect** command is not working and as a result local switching does not work. 2. For some images, the **no connect** command is not working to remove an existing connection.

  Conditions: The symptoms are observed with 3660 platform images where both ac_atm and atm_switching subsystems are responsible for local switching.

  Workaround: Remove ac_atm and use only atm_switching for local switching.

  Further Problem Description: Problems may arise for other 3660 platform images having both ac_atm and atm_switching.

- CSCsq10730

  Symptoms: A Cisco router may display the following messages after enabling the advanced signature set in IOS-IPS: Too many UUIDs in pdu type 0x0E Too many UUIDs in pdu type 0x0B Too many UUIDs in pdu type 0x0E Too many UUIDs in pdu type 0x0B

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(15)T, that is utilizing IOS IPS v5 feature, and is running with the advanced signature set (MSRPC). Symptom occurs when incoming MSRPC packets are malformed or do not comply with protocol.

Workaround: There is no workaround. The message is informational (cosmetic).

- CSCsq11620

  Symptoms: String handling is incorrect in the code which uses "strncpy" and "sprintf".

  Conditions: The symptoms are observed when accessing a specific string.

  Workaround: There is no workaround.

- CSCsq12337

  Symptoms: Parsing of a SIP message with MIME content fails, which causes call termination.

  Conditions: The symptoms are seen when the SIP message contains application/qsig or application/x-q931 contents in MIME without a Content- Length SDP header.

  Workaround: Add a Content-Length SDP header for application/qsig or application/x-q931 contents with appropriate value. Alternatively, disable sending application/qsig or application/x-q931 contents in the SIP message.

- CSCsq13348

  The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE.DNS engine. This vulnerability may cause a router to crash or hang, resulting in a denial of service condition.

  Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.

  NOTE: This vulnerability is not related in any way to CVE-2008-1447 - Cache poisoning attacks. Cisco Systems has published a Cisco Security Advisory for that vulnerability, which can be found at http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml.

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

- CSCsq14031

  Symptoms: Unable to ping IP address of session target. Packets of certain sizes (between 57 and ~63 bytes, depending on the type of packet) are corrupted when using a tunnel over a PPP multilink interface. EIGRP packets were within this range and so were dropped and caused the route to the IP address being pinged not to be added.

  Conditions: Issue may be related to encryption or Network Address Translation (NAT).

  Workaround: Disable or increase the value of **ppp multilink fragmentation**.

- CSCsq14210

  Symptoms: A router may crash when a ping is issued and when the **clear ip cef * prefix-statistics** command is issued on router.

  Conditions: The symptom is observed when encapsulation FR is configured on the dialer interface, having profile configuration, and CEF switching is also configured.

  Workaround: There is no workaround.

  Further Problem Description: When encapsulation FR is configured on the dialer interface having profile configuration, it was made as a CEF switchable interface by default. When the CEF looks for a fastsend vector, the vector was NULL and router crashes at this point. Encapsulation ppp has its own way of installing the punt adjacency when the call is not UP and then it makes the interface a CEF switchable interface when the call comes UP.

- CSCsq15496

  Symptoms: Auto-Upgrade Manager (AUM) crashes while downloading an ip base image.

  Conditions: The symptom is observed when AUM is used to download an ip base image.

Workaround: An upgrade to an ip base image can be done without using AUM. Use the manual method of upgrading to a new image.

- CSCsq15560

  Symptoms: In creating a multi-party video conference by calling into a Cisco IPVC MCU device, a call may intermittently suffer from one-way video.

  Conditions: The symptom is seen with a multi-party video conference which calls into a Cisco IPVC MCU device and where a local CME video endpoints calls the MCU via a gatekeeper over H323. This is a timing issue in the H.323 state machine. In a call flow, two sets of OLCs (for audio and video) are exchanged. BRQ is sent for audio OLC. Before BCF is received, GW gets video OLC. This updates the total channel bandwidth and checks if it is less then the approved BW. As it is not so, OLC is rejected resulting in one-way video.

  Workaround: There is no workaround.

  Further Problem Description: This scenario works fine with third party H323 endpoints with their own H323 stacks working with the same gatekeeper and MCU. A more heavily loaded (for instance, with debugs) CME gateway will experience the problem less often.

- CSCsq15994

  Symptoms: Low CPS may be observed.

  Conditions: The symptoms are seen with PPPoA and PPPoE sessions.

  Workaround: There is no workaround.

- CSCsq16611

  Symptoms: IPv6 packets are process switched instead of using Cisco Express Forwarding (CEF)

  Conditions: The above symptom is observed on a Cisco 7301 and Cisco 7200 routers.

  Workaround: There is no workaround.

- CSCsq18737

  Symptoms: A router may crash and tracebacks may be seen upon reconfiguring object-groups.

  Conditions: The symptoms are observed when the router is configured with an initial object-group configuration. If the object-group is reconfigured with two IP hosts, the router crashes.

  Workaround: There is no workaround.

- CSCsq18856

  Symptoms: Packets are not being switched by Cisco Express Forwarding (CEF).

  Conditions: This issue is seen on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsq18959

  Symptoms: Unable to configure percent police child policies below parent shaper policies.

  Conditions: Occurs when attempting to attach percent police child policy with parent shape policy. It should be allowed as shape rate provides the bandwidth.

  Workaround: Use fixed rate values rather than percent.

- CSCsq19047

  Symptoms: A VXML gateway may stop handling calls due to lack of memory. The memory leak occurs in Chunk Manager process.

Conditions: The symptom is observed on a VXML gateway that is running Cisco IOS Release 12.4(15)T and when the SIP Take back application is configured to initiate a REFER-based call transfer in a CVP scenario.

Workaround: There is no workaround.

Further Problem Description: Page 374 of this configuration & administration guide states how this configuration must be setup:
http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp4_0/configuration/guide/cvp40cfg.pdf

- CSCsq19231

  Symptoms: Wrong target shape rate for peak committed information rate (CIR).

  Conditions: Occurs when target shape rate is configured for the child policy.

  Workaround: There is no workaround.

- CSCsq19957

  Symptoms: A numbered access-group does not match traffic when configured under a class-map unless another matching criteria is added to the same class-map, which must be a non-numbered access-group match statement.

  Conditions: This has been observed for Gigabit ethernet on an NPE-G1, frame-relay encapsulated serial interface, and POS interfaces on a NPE-G2.

  Workaround:

  1. Add another match criteria under the same class, which has to be a non-numbered access-group such as **match ip dscp** or **match access-group<name>**. This triggers the numbered access-group to start matching traffic correctly.

  2. Have only one class defined plus class class-default under the policy-map, and it will classify traffic correctly.

- CSCsq20970

  Symptoms: On the 2432 platform UUT, the ’atm’ option is missing in the ’mode’ CLI when the T1 controller is being configured for ATM.

  Conditions: The symptom is observed on the 2432 platform with a T1 controller.

  Workaround: There is no workaround.

- CSCsq21347

  Symptoms: Sometimes WebVPN login page may not come up when a client browser connects to the gateway. Sometimes, login page may come up, but after entering the login credentials portal page does not come up. The following syslog messages are seen.

  1) We are able to enter the webvpn login page, but after entering the username and password, the page returns the error message "Internal Error" and does not let us login. Also, the traceback below is seen.

  ```
  May 10 06:15:19.183 PDT: %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 0 for chunk
  0, data 0 -Process= "SSLVPN_PROCESS", ipl= 0, pid= 265, -Traceback= 0x61898E8C
  0x6002DFC4 0x63D802FC 0x63D70C64 0x63D78A5C 0x63D79054 0x63D7986C 0x63D736A8
  ```

  2) The webvpn login page is not thrown up at all when we try to connect to the webvpn gateway. The ’Page is not displayed’ due to the following Traceback

  ```
  May 10 21:57:30.963 PDT: %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 0 for chunk
  0, data 0 -Process= "IP Input", ipl= 0, pid= 120, -Traceback= 0x61898E8C 0x6002DFC4
  0x63D6D564 0x63D72F48 0x63D5C804 0x62285B20 0x62288158 0x61F81940 0x61F83264
  0x61F8367C 0x61F83738 0x61F83980
  ```

Conditions: This can happen if WebVPN configuration is being removed and a client tries to connect.

Workaround: Avoid removing WebVPN configuration once it is configured.

- CSCsq24935

  Symptoms: A switch reloads when the **distance bgp** command is configured under ipv6 address family.

  Conditions: This symptom is observed on a Cisco 3560 that is running Cisco IOS Release 12.2(44)SE2. The same symptom is also seen on a Cisco 3750. The following commands are issued:

  router bgp <> address-family ipv6 unicast distance bgp <> <>

  The router subsequently reloads because of an Instruction access Exception.

  Workaround: There is no workaround. BGP/ipv6 is not supported on such platforms.

- CSCsq26111

  Symptoms: The extension number and speed dial number may not be displayed in full-length on a fallback ephone.

  Conditions: The symptom is observed after an ephone falls back to the SRST.

  Workaround: There is no workaround.

- CSCsq27365

  Symptoms: A router can crash at l2tp_process_control_packet_cleanup.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCsq29052

  Symptoms: Packets are not forwarded out from a point-to-point (P2P) interface.

  Conditions: The symptom is observed with CEF enabled and when the P2P interface is changed from an "ip unnumbered" configuration to another interface.

  Workaround: There is no workaround.

- CSCsq30717

  Symptoms: A NPE-G1 resets due to a hardware watchdog timeout. This is indicated in the **show version** output with "Last reset from watchdog reset".

  Conditions: The Cisco 7200 must have an enabled PA-MC-2T3-EC with channelized T1s.

  Workaround: Disable the PA-MC-2T3-EC.

- CSCsq31808

  Symptoms: With eiBGP multipath, incoming labeled packets may get looped in MPLS core instead of getting forwarded to CE, causing traffic issues. The following symptom may be found:

  - The error message below is frequently generated.

  ```
  Dec 17 07:44:46.734 UTC: %COMMON_FIB-3-BROKER_ENCODE: IPv4 broker failed to encode msg
  type 0 for slot(s) 0B -Traceback= 6044E470 60465864 6043BCFC 6043B570
  ```

  - The **debug cef xdr** command yields the following message:

  ```
  Mar 31 17:44:40.576 UTC: FIBrp_xdr: Table IPv4:<vrf name>, building insert event xdr
  for x.x.x.x/y. Sources: RIB Mar 31 17:44:40.576 UTC: FIBrp_xdr: Encoding path
  extensions ... Mar 31 17:44:40.576 UTC: FIBrp_xdr: - short ext, type 1, index 0 Mar 31
  17:44:40.580 UTC: FIBrp_xdr: Getting encode size for IPv4 table broker FIB_FIB xdr Mar
  ```

```
31 17:44:40.580 UTC: - short path ext: len 12 Mar 31 17:44:40.580 UTC: - short path
ext: len 24 Mar 31 17:44:40.580 UTC: - feat IPRM, len 12 Mar 31 17:44:40.580 UTC: =>
pfx/path 113 + path_ext 24 + gsb 8 + fs 16 = 161
```

- Checking the prefix, it points to drop entry.

```
router#show mpls forward vrf <vrf name> x.x.x.x Local Outgoing Prefix Bytes Label
Outgoing Next Hop Label Label or VC or Tunnel Id Switched interface 937 No Label
x.x.x.x/y[V]  0 drop <========= it is drop
```

- Checking the MOI flag of EBGP path, the No_Global flag (0x10) was incorrectly set.

```
router#show ip cef vrf <vrf name> x.x.x.x int [snip] path_list contains at least one
resolved destination(s). HW not notified path 70BFFC5C, path list 20E87B58, share 1/1,
type recursive nexthop, for IPv4, flags resolved MPLS short path extensions: MOI flags
= 0x16 <-------MOI flags 0x10 is incorrectly set (for ebgp path, correct flag should
be 0x4, 0x5, 0x6 ..) correct now. [snip]
```

Conditions: The eiBGP multipath is enabled; iBGP path comes up first , then the eBGP path. Both eBGP and iBGP paths could be in MPLS forwarding causing the issue.

Workaround: Using the **clear ip route vrf <name> x.x.x.x** clears the issue.

- CSCsq31958

  Symptoms: In a network with redundant topology, an Open Shortest Path First (OSPF) external route may remain stuck in the routing table after a link flap.

  Conditions: Problem observed in Cisco IOS Release 12.4T. Not present in Cisco IOS Release 12.3T.

  Workaround: The issue can be resolved by entering the **'clear ip route'** command for the affected route.

- CSCsq32443

  Symptoms: MCP rejecting Start-Control-Connection-Reply (SCCRP) with receive window size missing.

  Conditions: Occurs with peers that use or expect the default handling of RxWindowSize of (4) and do not include the attribute-value pair (AVP) in the SCCRQ/SCCRP messages.

  Workaround: Force peer to send AVP.

- CSCsq33509

  Symptom: Traceback@%SCHED-3-STUCKMTMR, Sleep with expired managed timer is seen while testing with CA servers.

  Conditions: The symptom is observed when running Cisco IOS Release 12.4 (19.18)T2.

  Workaround: There is no workaround.

- CSCsq34171

  Symptoms: A router may crash when the ip address/mask is changed on the interface.

  Conditions: The symptom occurs if EIGRP authentication is enabled.

  Workaround: Disable authentication.

  Further Problem Description: When the authentication is removed from the interface, the crash does not occur on changing the mask.

- CSCsq35036

  Symptom: An HWIC-1DSU-T1 card comes up with line loopback turned on.

  Conditions: The symptom is observed with Cisco 2801 and 1841 routers only.

  Workaround: Press the pushbutton to clear loopback condition.

  Alternate workaround: Execute the **clear service-module <>** command.

Further Problem Description: The problem happens because HWIC reset assert/deassert is not happening before and after the FPGA download respectively in these platforms.

- CSCsq36135

  Symptoms: A Cisco 3845 router may crash.

  Conditions: The symptom is observed when an SIP TNP phone with MWI configuration tries to register with the CME.

  Workaround: There is no workaround.

- CSCsq36269

  Symptoms: Packets being sent towards a Cisco 7200 that are group domain of interpretation (GDOI) encapsulated but which in fact the router wants to send out through the same interface (due to a routing problem) will not leave the router with the TTL decreased by one, but increased by one.

  As it is likely that the upstream router will send the packet again to the GDOI endpoint this will lead to a never-stopping flow of packets that will overwhelm the router.

  Conditions: Occurs when using GDOI on a Cisco 7200 and having a routing issue where the upstream router forwards packets towards the GDOI router, but the GDOI router wants to send the same traffic towards the upstream router.

  Workaround: There is no workaround.

- CSCsq36477

  Symptoms: The router crashes while executing the **no debug dmvpn** *condition* command.

  Conditions: Conditions unknown at this time.

  Workaround: There is no workaround.

- CSCsq37010

  Symptoms: Unable to set up SSL VPN full-tunnel from clients.

  Conditions: Occurs on Cisco 3845 router running the c3845-adventerprisek9-mz.124-19.18.T2 image. When Windows client attempts to connect, tunnel set up fails with error "The VPN client driver has encountered an error."

  Workaround: There is no workaround.

- CSCsq37349

  Symptoms: A router may crash due to a corrupted Program Counter.

  Conditions: The symptom is seen with Zone-based Firewall and IPS, along with VRF and IPSec tunnel configured.

  Workaround: There is no workaround.

- CSCsq37520

  Symptoms: A crash is seen when a child **policy-map** is added to a **policy-map** that is attached to a large number (1000s) of interfaces.

  Conditions: This symptom occurs when any configuration change results in the creation of 1000s of QoS queues at once.

  Workaround: Remove policy-map from all interfaces prior to modification.

- CSCsq38382

  Symptoms: Router crashes from console after the **privacy on** command is entered under **ephone1** when **no ephone 1** was issued from VTY line.

Conditions: Occurs when using both VTY and console.

Workaround: There is no workaround.

- CSCsq39244

  Symptoms: IPv6 traffic going to a 6PE device may be dropped after an interface flap.

  Conditions: The symptom is observed when the IPv6 prefix is known by BGP and the same prefix is assigned to the local interface. After an interface flap, the MPLS forwarded table is populated with drop and all incoming 6PE traffic going to that interface is dropped.

  Workaround: There is no workaround.

- CSCsq40088

  Symptoms: A Cisco 3845 router may crash when unconfiguring IPv6 nodes.

  Condition: The symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4T. The traceback is produced after configuring the **no ipv6 unicast-routing** command.

  Workaround: There is no workaround.

- CSCsq40572

  Symptoms: LLQ classification failed after configuring bandwidth in percentage.

  Conditions: This happens on a Cisco 3800 router loaded with Cisco IOS Release 12.4(19.18)T2.

  Workaround: There is no workaround.

- CSCsq40600

  Symptoms: When 802.1X is configured on the WAN interface of a Cisco 871, none of the "Spouse & Kids" related policy configuration works. In fact there is no access control applied on the port based on 802.1X authentication.

  Conditions: This only happens on the WAN interface of the 871 platform.

  Workaround: There is no work around for this as 802.1X isn't supported on the WAN interface of the 871 and therefore should not be configured on this interface.

- CSCsq40649

  Symptoms: Card is crashing while entries are being added to the access list.

  Condition: Occurs when additional entries are being added to an access list that is already attached to an interface. The card is crashing with memory corruption.

  Workaround: There is no workaround.

- CSCsq40659

  Symptoms: A client may not get a prefix when it has two relay agents on two interfaces of a single DHCP relay agent, with one of them being an unnumbered interface.

  Conditions: The symptom is seen on a router that is running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsq40813

  Symptoms: Queue-limit locked with the given value and remains dead with "random-detect discard-class-based."

  Conditions: Happens only with random-detect discard-class-based and queue-limit configuration.

  Workaround: There is no workaround.

- CSCsq41361

Symptoms: When the PIX initiates a phase 2 rekey, it sends the QM1 and the router responds with QM2 and immediately after that it sends IKE delete notify for the previous inbound SPI before receiving the QM3 from the PIX. The PIX after that sends the QM3 and the tunnel is rekeyed, but this causes the VPN tunnel to flap a bit and then PIX drops all TCP connections associated with that VPN tunnel.

Conditions: Occurs when PIX initiates a phase 2 rekey.

Workaround: There is no workaround.

- CSCsq41455

  Symptoms: The router hangs and has to be reset.

  Conditions: This crash happens when out-of-order sequence numbers are used in an ACL. In the ACL in the description, ACE 1 triggers the crash.

  Workaround: Instead of making the changes to the ACL with the ACL applied to the interface, if the changes are made to the ACL after it is removed from the interface, the crash will not happen.

- CSCsq41508

  Symptoms: An ACL with more than 13 ACEs will not show any matches on the OG ACEs.

  Conditions: If the ACL has more than 13 ACEs, any object group ACEs will not function properly.

  Workaround: There is no workaround.

- CSCsq42246

  Symptoms: Router crashes while reloading the satellite network module.

  Conditions: Occurs on a router running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsq42399

  Symptoms: Shortly after upgrade, the router shows the following error:

  ```
  May 22 09:05:53.109 METDST: %SYS-2-MALLOCFAIL: Memory allocation of 261116 bytes
  failed from 0x61A37948, alignment 0 Pool: Processor Free: 6427012 Cause: Memory
  fragmentation Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "Virtual
  Exec", ipl= 0, pid= 234, -Traceback= 0x61452110 0x6000A7FC 0x60010638 0x60010C2C
  0x634CB644 0x61A37950 0x61461910 0x 614BD940 0x6149E000 0x614C1B08 0x62AA2494
  0x62AA2478
  ```

  Traffic is affected, and the router unable to display output from the **show run**.

  Conditions: Occurs on a Cisco 7200 router running the c7200-adventerprisek9-mz.124-15.T3.bin. Service Selection Gateway (SSG) and RADIUS are involved.

  Workaround: There is no workaround.

- CSCsq43591

  Symptoms: When a session is cleared from the CPE and when it reconnects instantaneously, a ping fails to the CPE.

  Conditions: This symptom is observed under the following conditions:

  - LAC<->LNS setup. - Clearing of session from CPE. - In the **show pxf cpu vcci** command output, there is no VCCI present for the VAI. - Also seen in lab when the CPE is booted and the first session comes up.

  Workaround: Clear the VAI interface from the LNS. The session will reconnect and will work fine.

- CSCsq43831

Symptoms: A Cisco IOS router may unexpectedly reload when Forwarding Information Base (FIB) processes an adjacency for route that has many levels of recursion.

Conditions: This has only been seen after the following error message was displayed:

%COMMON_FIB-6-FIB_RECURSION: 10.10.10.1/32 has too many (8) levels of recursion during setting up switching info

Workaround: Change static routes so they specify both the interface and next-hop instead of just specifying the next-hop. For example change

ip route 10.0.0.0 255.255.255.255 192.168.1.1

to

ip route 10.0.0.0 255.255.255.255 GigabitEthernet1/0 192.168.1.1

This is particularly true when using eBGP between loopbacks to allow for multiple parallel links between the two eBGP peers, where one typically installs static routes for the eBGP peers address. Make sure these static routes have both interface and next-hop specified.

- CSCsq43934

  Symptoms: TCP/HTTP zone-based firewall (ZBF) session failed to established with dynamic or overload NAT mode.

  Conditions: Normal deployment condition.

  Workaround: There is no workaround.

- CSCsq44428

  Symptoms: Under certain conditions with IPv6 for EIGRP, the router may log error messages such as the following:

  ```
  00:00:09: %DUAL-3-INTERNAL: IPv6-EIGRP(0) 80: Internal Error
  ```

  Conditions: The error message is currently not causing a operational impact.

  Workaround: There is no workaround.

- CSCsq45734

  Symptoms: Router crashes while configuring match access-group name with long string.

  Conditions: Occurs when string length greater than 77 characters.

  Workaround: There is no workaround.

  ===

  New Condition: It can also happen with short string

- CSCsq45836

  Symptoms: Dynamic Multipoint VPN (DMVPN) shortcut tunnels may fail to get established on a DMVPN spoke running a phase 3 setup.

  Conditions: Occurs in Cisco IOS Release 12.4(20)T.

  Workaround: There is no workaround. However, data traffic would not be affected since the packets would take the spoke-hub-spoke path.

- CSCsq46742

  Symptoms: SIP gateway crashes when a 302 response contains a contact header with the same IP address as that of SIP gateway.

Conditions: The crash occurs only when the 302 response contains a contact header with an IP address the same as that of the gateway IP address. The crash also occurs only when the IP address is mapped to a domain name exceeding the length of the IP address received in the contact header.

Workaround: Ensure that the IP address that is received in the 302 response is mapped to a domain name not exceeding the length of the IP address.

- CSCsq46832

  Symptoms: The "IP SLAs: RTP VoIP Operation" feature was introduced in Cisco IOS Release 12.4(4)T to allow users to obtain some realistic VoIP Round Trip Time (RTT), Jitter, Packet Loss, and Mean Opinion Score (MOS) measurements from a live VoIP call over a real IP cloud and using a bonafide voice codec supported over voice DSPs. It has been found that in certain versions of the IOS 12.4T release train this feature is not functioning at all. The output of the **show ip sla statistics N** EXEC prompt command, where N is the IP SLA probe tag number, returns something similar to the following output reporting all zeroed-out measurements:

  ```
  VoiceGateWay#sh ip sla statistics 3 IPSLAs Latest Operation Statistics
  IPSLA operation id: 3 Type of operation: rtp Latest operation start time: 11:35:15.606
  EST Tue May 27 2008 Latest operation return code: No connection Latest RTT
  (milliseconds): 0 Source to Destination Path Measurements: Interarrival Jitter: 0
  Packets Sent: 0 Packets Lost: 0 Estimated R-factor: 0 MOS-CQ: 0.00 Destination to
  Source Path Measurements: Interarrival Jitter: 0 Packets Sent: 0 Packets Lost: 0
  Estimated R-factor: 0 MOS-CQ: 0.00 Operation time to live: 72083 sec Operational state
  of entry: Active Last time this entry was reset: Never
  ```

  Conditions: This behaviour is observed on Cisco Cisco 1700, 2600, 3700, 7200, 7500, 2800, and 3800 voice platforms installed with IOS 12.4(19.18)T or newer in the IOS 12.4T release family, and configured with the RTP VoIP IP SLA feature.

  Workaround: There is no workaround.

- CSCsq47043

  Symptoms: A Cisco router functioning as the standby for an Hot Standby Routing Protocol (HSRP) group way reload when it is dissociated from that group and then re-associated with it. A sample sequence of commands that may lead to the reload is:

  [Assume that the interface in question has been previously configured with **standby** *1* ip command.]

  ```
  Router(config)#interface g0/0.30 Router(config-subif)#no standby 1 ip
  Router(config-subif)#standby 5 ip 10.10.30.105
  ```

  // wait for a while.. then:

  Router(config-subif)#**no standby** *5* ip *10.10.30.105* Router(config-subif)#**standby** *1* ip

  Conditions: The reload is seen if the triggering commands are issued when the router is part of an interdevice redundancy system and its redundancy state is HOT_STANDBY and if interdevice redundancy tracks the HSRP state of the group to which the interface belongs (in other words, **scheme standby** <*group-name*> is configured under **redundancy interdevice** configuration.

  Workaround: Remove the **scheme standby** <*group-name*><noBmdBold> command from under the **redundancy interdevice** configuration prior to configuring the **standby** <*group number*> ip command on the interface. Also save configuration, reload and then re-apply **scheme standby** <*group-name*><noBmdBold> command.

- CSCsq47727

  Symptoms: Tracebacks seen when configuring on-board gigabit ports.

  Conditions: Occurs when the router and its on-board ports are configured from the Setup mode.

  Workaround: Do not use Setup mode to configure the on-board gigabit interfaces and other basic router parameters

- CSCsq48201

Symptoms: A crash may occur when creating a Bridge-Group Virtual Interface (BVI) while traffic is flowing.

Conditions: The crash could occur when a BVI interface is first created with the command **interface BVI** and traffic is being process switched by a physical interface in the same bridge-group. Once the BVI interface is created, subsequent **interface BVI** commands to configure that interface will not cause the crash.

Workaround: Remove the physical interface from the bridge-group, or prevent traffic from being process switch by the interface when the BVI interface is first created.

- CSCsq48717

  Symptoms: Attaching the following policy:

  ```
  policy-map p1 class prec1 class class-default shape
  ```
  will result in the packets to class prec1 not being enqueued to class-default.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(19.18)T02.

  Workaround: Remove the policy from the interface, remove class prec1, add the policy back and then add class prec1.

- CSCsq48949

  Symptoms: A hierarchical policy cannot be attached.

  Conditions: This symptom is observed with a Cisco 7200 router that is running Cisco IOS Release 12.4(19.18)T2.

  Workaround: There is no workaround.

- CSCsq49100

  Symptoms: Removal of last class-map before the qos-group class-map causes the router to crash.

  Conditions: Happens every time when the class-maps change from type(Mix) to type(Un-Mix), such as the following:

  ```
  Mix : dscp precedence qos-group
  Un-Mix: qos-group qos-group qos-group
  ```
  Workaround: There is no workaround.

- CSCsq49645

  Symptoms: No packets match in QoS match ACL test.

  Conditions: This condition is seen on a router loaded with Cisco IOS Release 12.4T images.

  Workaround: There is no workaround.

- CSCsq49768

  Symptoms: MAC L2TP clients failed to setup tunnel after L2TP network server (LNS) upgraded to Cisco IOS Release 12.4(19.18)T3.

  Conditions: Occurs when Mac OS X 10.4 and Mac OS X 10.5 clients attempt to connect to a LNS running Cisco IOS Release 12.4(19.18)T3. image loaded.

  Workaround: There is no workaround.

- CSCsq49816

  Symptoms: Adding a service policy to a PVC under switch subinterface with PPP multilink configured will cause PXF queue size to become misprogrammed.

  Conditions: Occurs when policy-map with priority class is attached to a MLP PVC under switch sub-interface and the MLP bundle is down. The PXF switch1 queue will be misprogrammed.

Workaround: Such a configuration is not allowed and has to be avoided.

- CSCsq50047

  Symptoms: A router may crash when a service policy is applied to a frame- relay map-class.

  Conditions: The symptom is observed when the minimum committed information rate (minCIR) is lowered causing an already attached policy to no longer have enough bandwidth. Then the service policy is removed and when it is reconfigured, the crash occurs.

  Workaround: There is no workaround.

- CSCsq50100

  Symptoms: When a call is placed between secure phone from SIP gateway to secure Cisco Unified CallManager (CCM) phone call is established as SRTP call. After hold/resume the call becomes non-secure.

  Conditions: All supplementary services are affected (hold/resume of a secure call, call transfer, conferencing, etc.).

  Workaround: There is no workaround.

- CSCsq51119

  Symptoms: A Cisco NHRP router may unexpectedly reload because of a bus error.

  Conditions: The router must be running NHRP, and the NHRP SNMP MIB must be enabled.

  Workaround: Disable the NHRP SNMP MIB. Save the configuration, and reload the router.

- CSCsq51158

  Symptoms: The signal of a Cisco 851w router may fluctuate.

  Conditions: The symptom applies to different environments where multi-path is more of an issue.

  Workaround: There is no workaround.

  Further Problem Description: A spectrum analyzer shows that the router has a signal of -60(+/-10)Db and that it stays at that level for about 7-10 seconds. It then drops by 40Db for 7-10 seconds before it restores itself to its original level.

- CSCsq51500

  Symptoms: When attempting to bring up the Secure Device Provisioning (SDP) Welcome page, the following message is displayed in the web browser: "IPv6 unicast-routing is not enabled".

  When using Internet Explorer, this is simply a cosmetic bug. With Firefox v2.0.0.14, this message gets displayed and the web page is corrupted and unusable so that SDP cannot continue.

  Conditions: When the config is saved and you do not have IPv6 unicast routing enabled, this problem sometimes occurs when attempting to display the SDP Welcome page.

  Workaround: Use Internet Explorer rather than Firefox.

- CSCsq51517

  Symptoms: QOS classification post-encryption is not working.

  Conditions: The symptoms are observed when using QoS post-classification (classification after encryption) of packets.

  Workaround: There is no workaround.

  Further Problem Description: With the changes introduced in CSCsq07294, Cisco IOS Release 12.4(20)T will no longer support QoS classification post-encryption.

- CSCsq51826

Symptoms: Router crashes when Flexible NetFlow for IPv6 is received and IPv6 fragmented packets are received.

Conditions: Flexible Netflow for IPv6 must be configured and fragmented IPv6 packets must be received.

Workaround: Deconfigure IPv6 Flexible NetFlow.

- CSCsq52048

  Symptoms: Router crashed while running **show vpdn tunnel all** command.

  Conditions: When there are thousands of L2TP tunnels coming up, going down, running **show vpdn tunnel all** may result in crash.

  Workaround: There is no workaround.

- CSCsq52847

  Symptoms: Connection establishment failed with the event agent.

  Conditions: Occurs when the Event Gateway is killed and restarted on a Cisco 1812 router while running Cisco IOS Release 12.4(19.18)T2.

  Workaround: There is no workaround.

- CSCsq54601

  Symptoms: SCCP and SIP registration fail with EzVPN and NAT configured. Only Voice traffic is affected

  Condition: Occurs when SCCP Registration traffic is passing through NAT Router.

  Workaround: There is no workaround.

- CSCsq55070

  Symptoms: Traceback occurs while testing AAA Authentication and Asynchronous Call (ACQ) feature.

  Conditions: Occurs on a Cisco 3745 running Cisco IOS Release 12.4 and Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsq55260

  Symptoms: Router crashes on issuing **no match vlan X** under class-map.

  Conditions: Occurs on a Cisco 2801 router running Cisco IOS Release 12.4(21.1)T.

  Workaround: There is no workaround.

- CSCsq56103

  Symptoms: Configuration issues occur on serial interfaces.

  Conditions: Two different issues occur:

  - When a strict policy is applied on a serial interface, if the user re-configures the strict priority configuration under the same class in the same policy, it will fail.

  - When the user tries to remove the service policy from the serial interface, The HQF data structure is not cleaned up. The class default BLT and physical interface BLT are not deleted.

  Workaround: There is no workaround.

- CSCsq57856

  Symptoms: When Cisco 2431 and Cisco 2691 router is configured with 1DSU-T1-V2 card, router crashes while loading.

Conditions: The crash is seen while loading the router, when router is configured with 1DSU-T1-V2.

Workaround: There is no workaround.

- CSCsq58748

  Symptoms: When a OCSP (Online Certificate Status Protocol) request is made for checking the revocation status for a certificate to the OCSP server, if under some circumstances the TCP connection for the OCSP request goes into a stalled state, then the IKMP process can get blocked. This can cause the router to be unable to process any further IKE packets, and can stop any new tunnel negotiations/rekeys/DPDs from occurring. Existing IPSEC SAs will continue to work until a rekey or DPD is triggered.

  Condition: Occurs on a Cisco IOS router with IPSec VPN and certificates and configured for revocation checking.

  Workaround: Perform the following steps: 1) Disable revocation checking and then reload. 2) Reload the router.

- CSCsq58779

  Cisco IOS devices that are configured for Cisco Unified Communications Manager Express (CME) and the Extension Mobility feature are vulnerable to a buffer overflow vulnerability. Successful exploitation of this vulnerability may result in the execution of arbitrary code or a Denial of Service (DoS) condition on an affected device.

  Cisco has released free software updates that address this vulnerability.

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

- CSCsq60750

  Symptoms: "Net Input" process can cause Cisco 2800 and Cisco 2811 routers to crash.

  Conditions: Occurs on the Cisco 2800 and Cisco 2811 routers when loaded with 12.4(19.18)T2.

  Workaround: There is no workaround.

- CSCsq60952

  Symptoms: Traffic is mis-classified when it arrives on a sub-interface and firewall is configured on the tunnel interface.

  Conditions: Occurs on routers running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsq61398

  Symptoms: L2TP/IPSec connections fail between Cisco 1800 clients and the Cisco 7200 server when the server is configured for hardware encryption.

  Conditions: Occurs with the following topology:

  User---1811 (LAC) F0/0 ------- Router--ASA---G0/1 c7200 (LNS)

  Occurs when Cisco 1800 routers are L2TP-over-IPsec clients, terminating their connection to a Cisco 7200. The problem exists in Cisco IOS Release 12.4(15)T3 and Cisco IOS Release 12.4(15)T4.

  Workarounds: Disable fast switching/CEF on the Cisco 7200. By entering the **no ip route-cache** command under both interface gig x/y and virtual-template xx of the Cisco 7200, the L2TP connection is stable.

  ```
  int Gig Ethernet X/Y no ip route-cache int virtual-template XX no ip route-cache
  ```

- CSCsq62269

  Symptoms: If a Cisco 3270 has no startup configuration, it will crash if the "autoinstall" option is selected.

  Condition: Occurs when there is no startup configuration and the router is using the c3270-adventerprisek9-mz.124-15.XZ.bin image.

  Workaround: Execute **tftpdnld -r in rommon to boot c3270-entbase-mz.124-15.XZ.bin**. Do not allow the "autoinstall" option to run. Save the default configuration and reboot it with the c3270-adventerprisek9-mz.124-15.XZ.bin image.

- CSCsq63041

  Symptoms: Xconnect may not be able to be configured if "ip address" has already been configured on the interface.

  Conditions: The symptom is observed when attempting to configure IPv6 protocol demux under xconnect, when "ip address" has already been configured.

  Workaround: There is no workaround.

- CSCsq63176

  Symptoms: PA-MC-T3/E3-EC PA does not pass full traffic after a sudden burst near line rate.

  Conditions: Occurs when 256 interfaces are configured on the port adapter with multilinks operating on those serial interfaces.

  Workaround: Configure fewer than 256 serial interfaces.

- CSCsq63278

  Symptoms: Shape rate under child policy is not met. Shape rate of child policy is equal to parent shape rate

  Conditions: Occurs on a Cisco 7200 router is running Cisco IOS Release 12.4(21.1)T.

  Workaround: There is no workaround.

- CSCsq63731

  Symptoms: If either the command **vlan-id dot1aq** *vlan-id* or the command **vlan-range dot1aq** *start-vlan-id end-vlan-id* is configured on a main interface which is also configured for routing, and an ARP packet is sent to the router on the configured VLAN, then the router may send an ARP reply with a VLAN ID of zero.

  Conditions: The symptoms are seen on a Cisco 2800 series and a Cisco 7200 series router when the command **vlan-dot1q** *vlan-id* is configured on the GigabitEthernet interface of a Cisco 2800 series router and **encapsulation dot1q** *vlan- id* is configured on the FastEthernet 2/1/2.1 interface.

  Workaround: Change the Cisco 2800 series router's (CE) configuration to use a sub-interface for the vlan-id instead of using the **vlan- dot1q** *vlan-id* command on the main interface. With a sub-interface configured on the 2800, we can verify that the ARP packets are sent with proper VLAN ID.

- CSCsq64663

  Symptoms: Router Crashes when EtherChannel is shut down

  Conditions: Occurs on a Metro Ethernet device with over 2000 IP SLA operations configured and CFM services defined for a EtherChannel. The **no int ether-channel ...** command causes the device to crash.

  Workaround: There is no workaround.

- CSCsq64843

  Symptoms: An IOS router configured with Dynamic Multipoint VPN (DMVPN) may run of memory.

  Conditions: The symptom may occur when hub or spoke is behind a NAT device.

  Workaround: There is no workaround.

- CSCsq67163

  Symptoms: Scheduling of IP SLA RTP operation crashes the router.

  Conditions: This problem occurs only when IPSLA RTP operation is configured and scheduled to run.

  Workaround: There is no workaround.

- CSCsq68388

  Symptoms: The router crashes while a console session configures "associate ccm 1 ..." under the "sccpccmgroup" submode after a concurrent VTY session configures the same "sccp ccm" group ID.

  Conditions: Cisco IOS routers with 12.4T support multiple user CLI sessions through Console or VTY for concurrent configuration, and this issue occurs when multiple users are present. Specifically, if one user enters the CLI parser-submode by command "sccp ccm group" and then another user removes the same ccm-group by command "no sccp ccm group" before the first user exits the submode, the router will crash if the first user enters a CLI command such as "associate ccm..." or "description ..." in that submode.

  A similar issue though not reported in this bug could also occur. For example, when multiple users are present, if one user enters the CLI submode with command "sccp ccm group 1" and then another user enters the CLI submode with command "sccp ccm group 2", it will make the first user's submode implicitly be working with sccp-ccm-group 2 instead of 1, which is incorrect. The fix here also resovles this similar issue.

  Workaround: Do not allow multiple users to configure the same sccp-ccm-group. Use the **show line** command to see if other users are configuring the router.

- CSCsq70248

  CSCsq70248

  This caveat fixes the wrong code (cc_patch issue) committed by CSCsm74168. See CSCsm74168 below.

  CSCsm74168

  Symptoms: Cisco Unified Border Element (CUBE) crashes when operating in SIP to SIP mode. This will happen if CUBE has received REFER on one leg and tries to send INVITE on the other leg as a part of a call-transfer.

  Conditions: Topology: [CRASH] Org.--(SIP Trk)--CSPS--(SIP Trk)--CUBE1--(SIP Trk)--CUBE2--(H323 Trk)--Term_1 | | (H323 Trk) | Term_2

  Call is established between Org. and Term_1 and the originator attempts to transfer the original call to a second party on the Term_2 side. When Term_2 answers, CUBE1 crashes.

  Workaround: There is no workaround.

  Further Problem Description: CUBE1 in detail: X-OR----------CUBE1--------(Term_1)X-EE----- | | | CUBE2 | | -----(Term_2)X-TO----------

X-EE and X-OR operate in SIP-SIP mode. When it tries to set up a new call to Term_2, it tries to get channels, xcaps, callParams info from the peer leg (the Term_1 leg is the peer leg for Term2). The Term_1 call leg passes channels, xcaps, but does not pass callParams details (that contains the operating mode). So the Term_2 leg takes the default and sets its mode as SIP- H323 and executes some of the H323 related function. The result is undefined and this leads to the crash.

- CSCsq70534

  Symptoms: A router crashes because of a block overrun (overwriting the memory block).

  Conditions: This symptom is observed only when templates are exported in the export packet, which is used in only version 9 of exporting.

  Workaround: Version 5 could be used for exporting.

- CSCsq70745

  Symptoms: Shape peak calculations are incorrect while configuring more than 10700000 bps on the interface.

  Conditions: Occurs when a policy-map is attached to interface.

  Workaround: There is no workaround.

- CSCsq70872

  Symptoms: Router crashes when executing the **clear zone-pair inspect session** command.

  Conditions: Occurs when the router has a TCP session active when the user executes the command.

  Workaround: There is no workaround.

- CSCsq74300

  Symptoms: Loopbacks, Null0, and other non-Point-to-Point interfaces are not allowed in a **route-map set** command because of the changes introduced with caveat CSCsk63775.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(18) or a later release. Upgrading to Cisco IOS Release 12.4(18) or a later release may break the existing network.

  Workaround: Use Cisco IOS Release 12.4(17) or an earlier release.

- CSCsq74307

  Symptoms: The PfR MC may reload.

  Conditions: This symptom is observed if the PfR BGP inbound feature is enabled, and inbound prefixes are configured and controlled by PfR, and the **clear ip bgp *** command is executed on the controlling BR.

  Workaround: Do not configure inside prefixes; instead, let PfR learn using the following configuration:

  oer master learn inside bgp

- CSCsq75526

  Symptoms: When DNS forwarding source interface is configured in a split DNS environment, the source address being populated in the packet while forwarding the DNS query is wrong. It always takes the first interface in the VPN routing/forwarding (VRF) view even when the DNS forwarding source interface is changed. DNS query fails.

  Conditions: The above symptom is seen on a router running Cisco IOS Release 12.4(15)T6.

  Workaround: There is no workaround.

- CSCsq75787

  Symptoms: Cannot enable AutoQoS on ATM subinterface.

Conditions: This happens on a Cisco 3800 router running Cisco IOS Release 12.4(15)T06.

Workaround: There is no workaround.

- CSCsq75944

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly. On the console or in the RP crashinfo file, the following message can sometimes be seen:

  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.

  Conditions: Occurs during normal use on a Catalyst 6500 or Cisco 7600. NetFlow must be enabled.

  Workaround: Disable Netflow by using one of the following commands on every sub-interface for which Netflow is configured:

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

- CSCsq76338

  Symptoms: Call across SIP trunk takes around 10 seconds to resume after called party goes on hold.

  Conditions: Occurs during normal operating conditions.

  Workaround: There is no workaround.

- CSCsq77043

  Symptoms: A Cisco IOS device configured for an Embedded Event Manager (EEM) Tool Command Language (TCL) policy that uses the TCL CLI library may have the policy hang if the devices hostname is longer than 20 characters long.

  Conditions: If the device is configured with a TCL policy that uses the **cli_open** TCL command and that device has a hostname longer than 20 characters the policy may hang.

  Workaround: Reduce the size of the hostname.

- CSCsq77968

  Symptoms: Changing the connect command configuration may reload the router.

  Conditions: Occurs when the same connection is configured twice with different interfaces and Data-Link Connection Identifiers (DLCI). This is observed when running the latest version of Cisco IOS Release 12.4T.

  Workaround: Instead of changing the connect command configuration, use the **no connect** command to remove the command and then re-apply the new connect command configuration.

- CSCsq78208

  Symptoms: The router is crashing during start up when NTP update is received from SUP.

  Conditions: Occurs when there is an NTP update and a Cisco Multi-Processor WAN Application Module (MWAM) is present.

  Workaround: There is no workaround.

- CSCsq78956

  Symptoms: Memory tracebacks and errors occur.

  Conditions: Occurs only when using IKE in 12.2SXH. May also occur in other IOS releases.

  Workaround: There is no workaround.

- CSCsq80546

  Symptoms: Router crashed when policy-map modified while passing traffic.

  Conditions: The problem was seen on Cisco routers running Cisco IOS Release 12.4(19.18T5).

Workaround: There is no workaround.

- CSCsq80658

  Symptoms: H325 call is not connected properly in Cisco Unified Border Element (CUBE).

  Conditions: In CUBE, tokens received in H225 CONNECT will be not passed to the other leg if the following CLI is enabled:

  voice service voip supplementary-service media-renegotiate

  Workaround: Disable the **supplementary-service media-renegotiate** command under **voice service voip**.

- CSCsq81073

  Symptoms: MGX RPM-XF backcard is reset when the **test rpm ecc 1bit** command is entered.

  Condition: Occurs on an MGX with two-port gigabit Ethernet and two-port POS backcards.

  Workaround: There is no workaround.

- CSCsq81116

  Symptoms: Router may reload when Optimized Edge Routing (OER) master configuration is **shut/no shut**.

  Conditions: Only occurs when OER master controller goes down and then rarely.

  Workaround: There is no workaround.

- CSCsq81235

  Symptoms: A VRF cannot be configured again when it is deleted by using the **no ip vrf** command.

  Conditions: This symptom is seen only on VRFs with an MDT tunnel.

  Workaround: There is no workaround.

- CSCsq83501

  Symptoms: Router crashes while configuring more than 256 channel-groups in PA-MC-2T3-EC

  Conditions: The crash is seen after configuring more than 256 channel-groups in PA-MC-2T3-EC.

  Workaround: Do not configure more than 256 channel-groups:

- CSCsq83872

  Symptoms: There may be a memory leak when the **no pppoe enable** command is applied.

  Conditions: This symptom is observed on a Cisco 831 router.

  Workaround: There is no workaround.

- CSCsq85615

  Symptoms: Phones stay registered to Cisco Survivable Remote Site Telephony (SRST) router and do not re-register to Cisco Unified CallManager (CCM) after connectivity is restored.

  Conditions: This problem affects only phones that use SIP/UDP for signaling. SIP/TCP and SCCP phones are not affected.

  Workaround: Reloading the phones will resolve this issue (temporarily, until the next loss of connectivity). To avoid the problem, do not configure IOS firewall on any router between a SIP/UDP phone configured for SRST and the CUCM.

  Further Problem Description: The problem is caused by IOS FW blocking the packets from the CCM that would notify the phone that the CCM is accessible.

- CSCsq86067

  Symptoms: Router will crash while configuring match access-group name with longer string.

  Conditions: Occurs when match access-group name is configured with string length greater than 122 characters.

  Workaround: There is no workaround.

- CSCsq87204

  Symptoms: A router may reload due to a crash after configuring the **no multi-path** command or the **shut** command.

  Conditions: This symptom occurs when the router is configured with Mobile IP, Mobile Router, and multipath on Cisco IOS Release 12.4(9)T.

  Workaround: There is no workaround.

- CSCsq88391

  Symptoms: Standby device configured for stateful switchover (SSO) continuously reloads.

  Conditions: The reload occurs as soon as the standby and primary devices are loaded with stateful switchover (SSO) configuration.

  Workaround: There is no workaround.

- CSCsq89122

  Symptoms: Cisco 7206VXR with NPE-G1, SA-VAM2+, and PA-A3-OC3MM may generate spurious memory accesses.

  Conditions: One possible trigger may be ATM link instability.

  Workaround: There is no workaround.

- CSCsq90567

  Symptoms: The TSP gets stuck in connected state.

  Conditions: Occurs after resuming an onhold shared DN from the associated ephone. The TAPI gets stuck.

  Workaround: There is no workaround except rebooting the ephone and the TAPI.

- CSCsq91342

  Symptoms: CUBE will truncate the Calling Number IE when passing through an MWI SETUP.

  Conditions: This symptom is observed in Cisco IOS Release 12.4T. Cisco IOS Release 12.3T works fine.

  Workaround: There is no workaround.

- CSCsq91788

  Symptoms: A Cisco 10000 series router crashes on loading negative configurations.

  Conditions: This symptom happens when loading provisioning/unprovisioning LS and/or PW connection scale configurations from TFTP while executing the **show xconnect all detail** command on other console.

  Workaround: There is no workaround.

- CSCsq91960

  Symptoms: VRF may not get deleted if the VRF NAME size is 32 characters on a dual RP HA/SSO router.

Conditions: This symptom occurs when adding a VRF with 32 characters on a DUAL RP HA router. (In some releases a VRF name with more than 32 characters will get truncated to 32.) The following may occur:

- There may be a DATA CORRUPTION ERRMSG. - While deleting this 32 character length VRF, VRF will fail to get deleted completely with an ERRMSG on active.

Workaround: There is no workaround.

- CSCsq92063

  Symptoms: Router may crash.

  Conditions: This symptom is observed when Flexible NetFlow is configured with a flow record that includes layer 4 fields and the flow monitor is applied to IPv6 traffic, and the traffic that FNF is monitoring has a payload length that does not allow us to reach the transport header in the IPv6 packet.

  Workaround: Configure Flexible NetFlow with a record that does not have any layer 4 (transport) fields.

- CSCsq93004

  Symptoms: Removal of a subinterface may cause memory corruption or a crash. The symptoms are unpredictable.

  Conditions: The symptoms are rare and will only be observed if a sub- interface is configured for **mpls traffic-eng auto-tunnel primary use**, and the sub-interface is later removed from the configuration.

  Workaround: Do not remove sub-interfaces.

- CSCsq93508

  Symptoms: When onboard hardware crypto is enabled and if an SSLVPN AnyConnect tunnel is brought up, tracebacks are continuously seen and no traffic will go through the tunnel.

  Conditions: The symptom is observed with hardware crypto enabled on a Cisco 1800 series router.

  Workaround: Enable software crypto.

  Further Problem Description: The issue is seen on an 1800 platform because other ISR routers do not handle SSL with a hardware engine; they use only software code for SSLVPN (even onboard crypto engine enabled).

- CSCsq93555

  Symptoms: MCT3 controller configuration is not saved properly and is lost on reload.

  Conditions: Occurs MCT3 controller is configured on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsq93564

  Symptoms: When Cisco 7965 and Cisco 7975 IP phones with add-on modules (7914/7915/7916) fall back to Cisco Survivable Remote Site Telephony (SRST), only 6 to 8 lines are available during SRST fallback.

  Conditions: This problem occurs when phones are registered on Cisco Unified CallManager (CCM) 6.1 fallback to SRST 4.3.

  Workaround: There is no workaround.

- CSCsq94677

  Symptoms: The second channel for a dual-line DN or the eighth channel for octo-line DN is not available for a fallback phone.

Conditions: This problem occurs when a phone falls back to the Cisco Survivable Remote Site Telephony (SRST) the second time after the SRST reboots.

Workaround: There is no workaround.

- CSCsr00711

  Symptoms: Cisco Unified Personal Communicator (CUPC) does not register with the server.

  Conditions: Occurs when Cisco IOS firewall is enabled on a router between the CUPC and the Cisco Unified Presence server. The CUPC is not able to register to the CUP server and consequently to Cisco Unified CallManager (CCM) either.

  Workaround: To avoid the problem, do not configure IOS firewall on any router between CUPC and CUP server.

- CSCsr00967

  Symptoms: A router crashes.

  Conditions: Clicking an application Citrix Server, for example a calculator, and, within a short period of time, clicking another application causes the router to crash.

  Workaround: There is no workaround.

  Further Problem Description: The router is crashing when a Citrix application is clicked and before it is launched another application is clicked. For the first application, the Cisco IOS gateway is waiting for a DNS resolution, and meanwhile TCP is closed, which is causing the appl_out_buffer of the corresponding context to be freed. Later, when the DNS resolution has come through, some data is attempted to be written to the server-side appl_out_buffer, and because it is null, the router is crashing.

  ```
  buffer==NULL check was missed in the function sslvpn_http_write_start_chunk before
  filling some data into it.
  Buffer NULL check is added in sslvpn_http_write_start_chunk function before accessing
  the buffer.
  ```

- CSCsr02593

  Symptoms: Incoming call incorrectly rings Skinny Call Control Protocol (SCCP) overlay.

  Conditions: An incoming call for DN 2 rings both SCCP phone A, which has the DN and another SCCP phone B without it but has an overlay line. DN 2 and overlay line aren't shared line. Incoming call for the overlay only rings the overlay but incoming call for DN 2 will ring both.

  Workaround: Remove the overlay button from phone B, restart it, make an incoming to DN 2, add the overlay button back, restart phone. However, the problem will happen again after reload.

- CSCsr02848

  Symptoms: QoS policy is not getting attached to PPPATM session through virtual template.

  Conditions: This symptom is observed in a Cisco IOS Release 12.4(20)T image.

  Workaround: There is no workaround.

- CSCsr03713

  Symptoms: Secure Real-Time Transfer protocol (SRTP) calls failing.

  Conditions: Occurs with the following topology:

  OGW---srtp,sip-----TGW

  When SRTP is disabled, calls are passed.

  Workaround: Fall back to RTP.

- CSCsr06282

  Symptoms: Causes router to reload following a SNMP get operation.

  Conditions: Only occurs when a DHCP operation is configured with option-82 parameters.

  Workaround: Do not query MIB objects relating to the DHCP operation configured with option-82

- CSCsr08750

  Symptoms: A router may crash.

  Conditions: The router will crash with IO memory corruption when the **memory reserve critical [1-5]** command is executed.

  Workaround: Configure the **memory reserve critical** command with a much greater size.

  Further Problem Description: This issue occurs only when the ratio of free processor memory and free IO memory is high (say greater than 90).

- CSCsr09062

  Symptoms: Cisco 7200 crashes due to memory corruption.

  Conditions: Occurs when MLP+QoS is configured on a Cisco 7200 router. QoS policy is having bandwidth, change the BW parameter and flap the multilink using **clear int multilink1** to see the crash.

  Workaround: There is no workaround.

- CSCsr09400

  Symptoms: The packets decrypted with VSA hardware encryption and with CEF enabled while using L2TP protected by IPsec are not switched correctly.

  Conditions:

  1. Using the router as an L2TP termination hub.

  2. Using hardware encryption, specifically the VSA hardware engine.

  3. Using CEF switching.

  Workaround: There are several possible workarounds:

  - Disable CEF.

  - Apply the crypto map on the corresponding virtual-template interface alongside the physical interface.

  - Remove and reapply the crypto map (works until the next reboot).

  - Configure the **no ip route-cache** command and then the **ip route-cache cef** command on the virtual-template interface.

  Further Problem Description: If this issue is reproduced in lab conditions, and the **debug ip packet detail** command is enabled, the following can be seen in the debugs:

  ```
  *Jul 1 04:43:49.183: CEF: Try to CEF switch 10.175.135.48 from Virtual- Access2
  ```
  The address in this message is "bogus" and corresponds to the data within the packet before the decryption, which essentially contains random bytes, so it can be anything.

- CSCsr10075

  Symptoms: Under very rare timing condition, an OSPF Type-5 route may stay in the routing table after the adjacency is lost over ISDN/virtual-access interface.

  Conditions: The problem is seen only in Cisco IOS versions that do not have integrated CSCeh23420. Cisco IOS versions with CSCeh23420 are not affected.

Workaround: Clear IP route for the route, which is stuck in the routing table. Upgrade to a Cisco IOS version that are integrated with CSCeh23420 or CSCsr10075.

- CSCsr10221

  Symptoms: Hub router may crash after establishing 250 or more IPSec tunnels.

  Conditions: The symptom is observed with 250 or more DMVPN tunnels with traffic flowing in them. It is seen when a QoS service policy is associated with the spokes which are up.

  Workaround: There is no workaround.

- CSCsr10335

  Symptoms: A router loses its default gateway during autoinstall.

  Conditions: This issue was seen on Cisco IOS Release 12.4(15)T5, but should affect every Cisco IOS version.

  Workaround: 1. Manually do a **shut** followed by a **no shut** on the interface. 2. Create an EEM script, for example:

  event manager applet Check-Default-Route event syslog pattern "CNS-3-TRANSPORT: CNS_HTTP_CONNECTION_FAILED" action 1.0 cli command **enable** action 1.1 cli command **config term** action 1.2 cli command **interface GigabitEthernet0/0** action 1.3 cli command **shut** action 1.4 cli command **no shut** action 1.5 cli command **end** action 1.6 cli command **write** ! end

  3. In network-confg, configure "ip address dhcp" for the interface which is supposed to get the default gateway from DHCP.

  interface *interface_name* **ip address dhcp** end

- CSCsr11449

  Symptoms: The ingress decrypted packets do not get through with L2TP/IPSEC, even though they show up in the "decrypted" counter of the **show crypto ipsec sa** command output.

  Conditions: This symptom is observed when the **set nat demux** command is configured under the crypto map entry and when L2TP over IPSEC termination is used. VSA is used as the crypto engine.

  Workaround: There is no workaround.

- CSCsr12476

  Symptoms: Incrementing output queue drops on mGRE tunnel interface.

  Conditions: This symptom is observed on a Cisco 7206 NPE-G2 router that is running Cisco IOS Release 12.4(15)T6. This same symptom is not observed on a Cisco 7206-NPE-G1 that is running the same code.

  Workaround: There is no workaround.

- CSCsr12874

  Symptoms: MR reloads when unconfiguring **ipv6 router nemo** at gotoMRIPV6State.

  Conditions: The symptom is observed when MR is registered and **no ipv6 router nemo** is configured.

  Workaround: Do not configure/unconfigure **ipv6 router nemo** on MR.

- CSCsr14879

  Symptoms: The device crashes when it boots up.

  Conditions: Occurs on a router running the svcmwam-g8is-mz image.

  Workaround: There is no workaround.

- CSCsr15478

  Symptoms: An input wedge is observed on an interface, when multicast traffic is flowing.

  Conditions: The symptom is observed in a DMVPN hub-spoke scenario with a point-to-multipoint (P2MP) GRE tunnel having tunnel protection configuration. When multicast traffic flows from hub to spoke through these tunnel interfaces, the incoming interface of the hub is getting wedged and even the ping to peer stops working.

  Workaround: There is no workaround, other than reloading the router.

- CSCsr16693

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

  Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

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

- CSCsr17429

  Symptoms: The build breaks after the commit of CSCsk39308, which brings IP CEF related enhancement into dialer.

  Conditions: The basic images do not include IP CEF subsystems. Hence, when we try to build them, the references to IP functions are not resolved.

  Workaround: There is no workaround.

- CSCsr18200

  Symptoms: A busy tone is not heard when a 183 message is received before a 4xx busy message.

  Conditions: SIP trunk architecture with soft switch. This bug affects both 12.4(15)T and 12.4(11)XW software releases.

  Workaround: A patch is required, forcing the media off when a busy message is received.

- CSCsr20566

  Symptoms: A router may log SCHED-3-STUCKMTMR for Dampening process, after which point all dampened interfaces will be permanently dampened from a routing-protocol viewpoint.

  Conditions: This symptom is observed when multiple interfaces are configured with dampening feature.

  Workaround: There is no workaround.

- CSCsr20889

  Symptoms: The system reloads.

  Conditions: The symptom is observed when a dynamic crypto map is added to the existing GETVPN crypto map with a different sequence.

  Workaround: There is no workaround.

- CSCsr22077

  Symptoms: When an interface is attached with the same crypto map as an existing crypto map, the crypto map is able to be deleted, when it should not be.

  Conditions: The symptom is observed when a crypto map is applied to an interface and is then deleted. Although the crypto map is deleted (but is not showing), the user will still see the following warning message:

  Crypto-map <crypto map> is in use by interface(s): <interface> Please remove the crypto map from the above interface(s) first

  Workaround: Always remove the crypto map from the interface before deleting the crypto map.

- CSCsr24071

  Symptoms: Uninitialized variables can lead to bad quality of code in the IOS code base.

  Conditions: These errors can cause a synchronization damage leading to a build failure. The files affected include: cifs_api.c sslvpn_trie_scan.c sslvpn_tunl_ios.c sslvpn_vw_ctx.c

  Workaround: There is no workaround.

- CSCsr24421

  Symptoms: A router may crash for GetParameterNames RPC, with NextLevel set to "FALSE".

  Conditions: The symptom occurs for objects without instances, i.e., objects with read access.

  Workaround: GetParameterNames with NextLevel True of objects can be used to obtain the first level objects and parameters. Again, GetParameterNames of the first level objects can be used to know the supported objects and parameters. This is, however, a lengthy process.

- CSCsr24997

  Symptoms: There is an uninitialized variable used in stile_api.c which is triggering a compilation warning.

  Conditions: The symptom is observed when an uninitialized variable is triggering a compilation warning: ../stile/stile_api.c: In function ‘stile_populate_protocol_list_entry’: ../stile/stile_api.c:341: warning: ’type’ might be uninitialized in this function.

  Workaround: There is no workaround.

- CSCsr27305

  Symptoms: A Cisco 1801 router withdraws power to Polycom 430 IP phone and phone power cycles continuously.

  Conditions: The symptom is observed with a Cisco 1801 router with POE-180x daughter card and external power module with default switchport configuration that powers a Polycom 430 IP phone. CDP is enabled so that phone can detect Voice VLAN. The phone requests 4.5W of power and the router is only giving 4W.

  Workaround: Turn off CDP on switchport.

  Further Problem Description: The same Polycom IP phone works correctly on any DSBU POE switch.

- CSCsr29468

  Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

- CSCsr31518

  Symptoms: File copy is not working through FTP and the following error is seen:

  ```
  %Error opening ftp://USERNAME:PASSWORD@FTP-SERVER//SOURCE_FILE DESTINATION_PATH
  (Incorrect Login/Password)
  ```
  Conditions: The symptom is observed when FTP protocol is used for copying.

  Workaround: Add one more character to the password. Since this defect will drop the last character of the password, a dummy character will workaround this issue. For example, if the password is "1234", use "12345".

- CSCsr41239

  Symptoms: There may be spurious memory access when configuring **default ipv6 address** with "eui-64" as the interface identifier under dialer interface configuration mode.

  Conditions: The symptoms are observed when configuring **default ipv6 address** *ipv6 add* **eui-64** under "interface dialer 1". This happens only when CDP is enabled.

  Workaround: Disable CDP before configuring the router.

  Further Problem Description: When a packet with an "ADDR_ILLEGAL" address is received, it is processed by finding the next-hop address. This causes the spurious memory access. There is no functional impact.

- CSCsr44967

  Symptoms: When registering a multi-event Tool Command Language (TCL) policy in the Embedded Event Manager (EEM), the registration will fail with the following error message:

  ```
  %HA_EM-6-FMPD_EEM_LOG_MSG: Register event failed: Only correlate and attribute
  statements are allowed within trigger
  ```
  Conditions: The symptom is observed on all multi-event TCL policies in EEM 2.4 when the trigger block contains a closing brace that is by itself on a line. For example:

  ```
  ::cisco::eem::trigger { ::cisco::eem::correlate event e1 or event e2 or event e3 or
  event e4 ::cisco::eem::attribute tag e1 occurs 1 ::cisco::eem::attribute tag e2 occurs
  1 ::cisco::eem::attribute tag e3 occurs 1 ::cisco::eem::attribute tag e4 occurs 1 }
  ```
  Workaround: Add a space to the beginning of the line with the closing brace of the trigger block:

  ```
  ::cisco::eem::trigger { ::cisco::eem::correlate event e1 or event e2 or event e3 or
  event e4 ::cisco::eem::attribute tag e1 occurs 1 ::cisco::eem::attribute tag e2 occurs
  1 ::cisco::eem::attribute tag e3 occurs 1 ::cisco::eem::attribute tag e4 occurs 1 }
  ```
  Further Problem Description: This will not impact customer network and traffic.

- CSCsr45653

  Symptoms: CEF entry is not deleted when its neighbor is deleted.

  Conditions: The symptom occurs when netflow is configured.

  Workaround: There is no workaround.

  Further Problem Description: This issue affects memory management which in turn may impact performance.

- CSCsr46333

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

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.4(20)T. This problem has been seen on only one router, and it happened only once. At this stage, the root cause has not been identified. This enclosure will be updated as more information is gathered.

  Workaround: There is no workaround.

- CSCsr46367

  Symptoms: When registering an Embedded Event Manager (EEM) Tool Command Language (TCL) policy that has multi-event correlation for just track objects, the EEM system may get into an inconsistent state where a previously registered TCL policy will not be triggered, unregistered, or reregistered. This is seen when the following error is printed while registering the problematic policy: Embedded Event Manager configuration: failed to register the event spec for policy all_track.tcl: requested function is not supported

  Conditions: The symptom occurs only if the event manager server returns an error while trying to register an event. In this case the error is "function is not supported" because a multi-event TCL policy must have at least one event in the correlation statement.

  Workaround: Do not try to register a policy that is unsupported.

- CSCsr48828

  Symptoms: A Cisco router may display the following traceback: %SYS-2-GETBUF

  Conditions: The symptom occurs when ACLs are configured on the WAN interfaces of the router. When outbound packets fail and are dropped on an outbound ACL, a traceback is generated. If the packets are stopped or the ACLs removed, the tracebacks stop. The problem is seen with the VSA accelerator, but not seen when software crypto is used.

  Workaround: There is no workaround.

- CSCsr49316

  Symptoms: A crash happens when the **show ipv6 rpf x:x:x::x** command is given.

  Conditions: This symptom is observed only when there are more than 16 adjacencies for a single static route. The crash happens when the **show ipv6 rpf** command is given for this particular static route.

  Workaround: There is no workaround. This problem occurs as long as there are more than 16 adjacencies for single static route even if some of them are not active.

- CSCsr50548

  Symptom: The zone-based firewall is dropping conference calls.

  Conditions: Make a conference call within the CCM. Conference resources are available out of the box, where the firewall is configured between the CCM and the conference resource GW. These conference resources are registered with CCM. Registration traffic is seen via the Skinny protocol. During a conference call, logs show that the firewall is dropping media packets.

  Workaround: There is no workaround.

- CSCsr50821

  Symptoms: A router may crash when ARP hits through interrupt level.

  Conditions: This symptom is observed when bridging is configured, but it may also be observed when the ARP code hits by interrupt context, which is unpredictable.

  Workaround: There is no workaround.

  Further Problem Description: This defect was introduced via CSCsq05997. Cisco IOS Release 12.4 and 12.4T are not affected by this defect, but Cisco IOS Release 12.2S may be affected by this defect.

- CSCsr55278

  Symptoms: Fast switching of multicast packets may not occur on the interface of a PE router. All multicast packets are forwarded in process switching.

Conditions: The symptom is observed after the interface is changed from a forwarding interface of one VRF to another VRF.

Workaround: There is no workaround.

- CSCsr55713

  Symptoms: A crash occurs.

  Conditions: The crash is caused by a ping across an ISATAP tunnel. The symptom is observed only in Cisco IOS Release 12.4(15)T7 on the Cisco 7200 (it is not known to affect other platforms), since the crash is dependent on the Cisco IOS memory map (which varies with each image).

  Workaround: There is no workaround.

- CSCsr55970

  Symptoms: A router may crash due to a bus error.

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(20)T with an IOS firewall.

  Workaround: There is no workaround.

- CSCsr56105

  Symptoms: A Cisco IOS VoIP gateway may experience audio issues such as dead- air or one-way audio for VoIP call present on the gateway. When this occurs, the following error message will be displayed on the gateway: %C5510-1-NO_RING_DESCRIPTORS: No more ring descriptors available

  Conditions: The symptom is observed on a Cisco 2801 VoIP gateway that is running Cisco IOS Release 12.4(20)T or Release 12.4(15)XZ1.

  Workaround: There is no known workaround to prevent this issue while using Cisco IOS Release 12.4(20)T or 12.4(15)XZ1 while using the Cisco 2801 router. Use an earlier release to avoid this issue.

- CSCsr56699

  Symptoms: A router crashes.

  Conditions: When invoking call features (hold, transfer, conf) on a CME router where the AIM-IPS-K9 (inline and prom) is configured on the tunnel interface, the router crashes due to a software-forced crash (corrupted next pointer blk) with a buffer overflow.

  Workaround: There is no workaround.

  Further Problem Description: How to reproduce the problem:

  1) IP phone A from Call Manager calls IP phone B belonging to the Cisco 3825 CME. 2) Activating the call transfer button of IP phone B can crash the Cisco 3825 router.

  The normal call setup from the CM to the CME seems to be working fine.

  Other specifications:

  1) The problem can be reproduced without FW. 2) The crash is reproduced with ids mon configured on the tunnel only (need not be on the G1/0.150 as in the original setup). 3) Crash is reproduced in both promiscuous mode and inline mode. When ids mon is configured on the tunnel with one call up, simply put, the call on hold and the router will crash within a few seconds. 4) The router does not crash if running in process mode. 5) The crash is reproducible. 6) The crash occurs if inline and bypass mode is configured. 7) This problem was found during follow-up workaround testing for CSCsq51416 where simple call is not able to complete if ids mon inline is configured only on the switch interface.

- CSCsr57815

  Symptoms: Unable to attach a VC class to ATM sub-interface after unconfiguring **mpls experimental 1**.

  Conditions: The symptom occurs with a Cisco 7200 series router.

  Workaround: There is no workaround.

- CSCsr58052

  Symptoms: TCP packets with the Explicit Congestion Notification (ECN) bit turned on may be dropped by the Zone Based Firewall (ZBF), and the connection will not be established.

  Conditions: The symptom is observed when the TCP ECN bit is set on a new TCP connection in either direction (inbound or outbound) through the ZBF on the route.

  Workaround: Use Cisco IOS Release 12.4(15)T or earlier, as these releases are not affected.

  Further Problem Description: TCP ECN is described in RFC3168.

- CSCsr59242

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

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

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

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

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

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

- CSCsr59719

  Symptoms: A router may crash soon after configuring **cns config initial**.

  Conditions: The symptom is observed when configuring **cns config initial** with an invalid IP address for the status URL, for example:

  ```
  router(confif)#cns config initial <any non-existent ip address> status
  http://1.1.1.1.1.1.1/junk
  ```

  When the connection to the initial server fails, the status message is posted to the status URL which will cause the router to crash if the IP address is invalid.

  Workaround: Ensure the configured ip-addresses are valid.

- CSCsr64843

  Symptoms: A Cisco 1805 router may hang during reload.

  Conditions: The symptom is observed during the platform reload. After self- decompressing the image, the router goes to hang state.

  Workaround: There is no workaround.

- CSCsr67788

  Symptoms: IPv6 traffic is classified as IPv4 traffic.

Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(20)T.

Workaround: There is no workaround.

- CSCsr70197

  Symptoms: A router running Dynamic Multipoint VPN (DMVPN) may crash.

  Conditions: The symptom is observed when trying to unconfigure an MGRE tunnel interface running Next Hop Resolution Protocol (NHRP).

  Workaround: There is no workaround.

- CSCsr71715

  Symptoms: Call bubble may be missing, ringing LED not on, and Caller ID shows unknown.

  Conditions: The symptoms are observed after a hardware conference initiator parks or transfers the hardware conference call.

  Workaround: There is no workaround.

- CSCsr73786

  Symptoms: Router may crash or tracebacks may be seen.

  Conditions: The symptoms are observed when the **show crypto pki trustpoints status** command is used.

  Workaround: There is no workaround.

- CSCsr73798

  Symptoms: Traffic generated locally on the router in IVRF going to FVRF does not hit the crypto map and does not get encrypted. If the traffic arrives to the router from IVRF everything works fine and packets are encrypted.

  Conditions: The symptom is observed when a crypto map is terminated in a front VRF in a router rather than in a global routing table. It is seen with packets generated locally on the router from an inside VRF that go to an outside VRF, and where there is a matching crypto map.

  Workaround: There is no workaround.

- CSCsr80601

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

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

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

- CSCsr82003

  Symptoms: With a setup that has two routers receiving the same 300 multicast traffic from a video headend, if one of the links to the headend fails, about half of the multicast groups are blacked out as the RPF information for some of the sources is set wrong. Additionally, if both of the links are lost, we still have entries in the multicast routing table as the alternate route is used as the traffic incoming interface.

  The IGP is OSPF, with area0 in the core, and area 1 (to be set to stub soon) on the headend connecting links. There is MPLS TE with multicast-intact command under OSPF on the routers.

  Conditions: The problem happens when one of the headend connecting links is lost.

  Workaround: Remove the **ip multicast multipath** command from the two routers to disable ECMP load-splitting.

- CSCsr85766

  Symptoms: After an IP SLA operation finishes, all status variables that are expected to be conserved until the next operation become “Unknown.”

  Conditions:

  – If there is timezone offset and the local time date is advancing to the UTC date.

  – Found in Cisco IOS Release 12.4(20)T.

  Workaround: Schedule the operation so that it starts on the UTC date and the local date configured by the **clock timezone** command becomes the same.

- CSCsr87229

  Symptoms: Callers that use a caller-ID length of 15 characters or greater cannot call out of analog MGCP ports.

  Example:

```
MGCP Packet received from --->
CRCX 132 AALN/S0/SU1/0@nicmatth-ipipgw MGCP 0.1
C: A0000000010000260000000F5
X: 23
L: p:20, a:PCMU, s:off, t:b8
M: recvonly
R: L/hd
S: L/rg, L/ci(08/08/15/44,1002,This is my long name)
Q: process,loop
<---

MGCP Packet sent to --->
510 132 unsupported caller id length
```

  Conditions: The BELLCORE standards support only 15 characters, and the MGCP gateway disconnects the call because of unsupported caller-ID length and displays the following message:

  510 unsupported caller id length.

  Workaround: Configure a caller ID less then 15 character, or use the port with SCCP or H323 to prevent this. Also, the following cptones are not affected: “FR”, “DE”, “NO”, “IT”, “ES”, “ZA”, “TR”, “GB”, “AT”.

- CSCsr87466

  Symptoms: An outgoing INVITE from the Cisco IOS sip stack with SDP and authorization configured over the SIP trunk is failing because of an incorrect Response field generated within the Proxy Authorization header when the auth-int method is used as QOP. The Cisco IOS sip stack does not include SDP message body in the md5 hash calculation.

  Conditions: This symptom is observed under the following conditions:

  – Cisco IOS sip stack.

  – The auth-int method is used.

  – The outgoing INVITE packet contains SDP body.

  Workaround: Potential workarounds are to:

  – Disable early offer (not sure how to do it on IOS sip-ua).

  – Use the auth method instead of the auth-int method. This should work if the incoming Proxy Authorization reply contains only the auth method.

- CSCsr93254

  Symptoms: Build breakage with wan/nhrp.c.

Conditions: The symptom is observed when wan/nhrp.c is used.

Workaround: There is no workaround.

- CSCsr93416

  Symptoms: The reflexive ACL implementation is broken (evaluated traffic is dropped by the return ACL).

  Conditions: This symptom is observed with Cisco IOS Release 12.4(20)T and only if the ACL with evaluate ACE (rule) has fewer than 13 ACEs (rules).

  Workaround: Add dummy rules (ACEs) to the ACL with an “evaluate” statement so that the number of rules (ACEs) in the ACL is greater than 13.

- CSCsr94563

  Symptoms: When registering an Embedded Event Manager (EEM) policy in a scheduler class that has no threads allocated to it, EEM will produce the following error message:

  ```
  %HA_EM-4-FMPD_NO_SCHED_THREAD: No threads are configured to service event class
  ```
  When attempting to unregister the policy, EEM may produce the following error and the policy will not be unregistered:

  ```
  EEM configuration: failed to unregister the event spec for policy policyname: unknown
  event ID
  ```
  In addition, a triggered event will not actually run once this problem is experienced.

  Conditions: This symptom is observed in images with the fix for CSCsr46367 and support for different scheduling classes in the EEM server.

  Workaround: First allocate some threads to the class, and then configure the policy in that class.

  Further Problem Description: This problem affects both Tcl-based policies and applets.

- CSCsu00313

  Symptoms: SRTP call fails through IP-IP gateway with SIP end points.

  Conditions: SRTP call may fail with SIP trunk in between two CUCMs that are connected through IP-IP gateway.

  Workaround: There is no workaround.

- CSCsu02176

  Symptoms: A router reloads continuously on switching off one of the redundant power supplies.

  Conditions: This symptom occurs when a router reloads continuously on switching off one of the redundant power supplies.

  Workaround: There is no workaround.

- CSCsu04446

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

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

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

  ```
  oer master
   learn
    prefixes 100
  ```

- CSCsu10606

  Symptoms: A device crashes with the following error message: Breakpoint exception, CPU signal 23, PC =0x606CE1B4

  Conditions: The symptom is observed during Online Certificate Status Protocol (OCSP) use.

  Workaround: There is no workaround.

- CSCsu22997

  Symptoms: Right after the **show ephone summary** command is executed, the device crashes because of a bus error (CPU signal 10).

  Conditions: This symptom is observed on a Cisco 2811 that is running Cisco IOS Release 12.4(20)T with an ephone.

  Workaround: There is no workaround.

- CSCsu24087

  Symptoms: A router hangs for a couple of minutes, then crashes anytime the **clear ip bgp neighbor x.x.x in** or the **clear ip bgp neighbor x.x.x out** commands are issued.

  Conditions: This issue is being experienced in a Cisco 7609 that is running Cisco IOS Release 12.2(33)SRB3.

  Workaround: Suggested CU to avoid the use of that command or try only with the **clear ip bgp neighbor** command without **soft in**.

- CSCsu30540

  Symptoms: HWIC-4SHDSL: 4Wire annex F with coding 16-TCPAM link goes down after the **shut** command followed by the **no shut** command.

  Conditions: This symptom occurs after the 4WIRE SHDSL card with annex F coding 16-TCPAM configuration goes down after the **shut** command followed by the **no shut** command and never comes up. This issue is seen only with annex F coding 16-TCPAM, enable annex on CPE first and then CO side. This issue is not seen on 4WIRE SHDSL card with annex G coding 16-TCPAM.

  Workaround: There is no workaround.

- CSCsu31042

  Symptoms: A small memory leak may occur.

  Conditions: This symptom is observed when a PPPoE client or a PPPoA client is configured.

  Workaround: There is no workaround.

- CSCsu31954

  Symptoms: A router reloads.

  Conditions: Under certain crypto configurations with NetFlow also configured, the router will reload when required to fragment CEF-switched traffic on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsu32104

  Symptoms: A PRE-3 that is running Cisco IOS Release 12.2(31)SB code may encounter a Redzone overrun memory corruption crash.

  Conditions: Unknown at this time.

  Workaround: Turn off “Auto IP SLA MPLS” by entering the **auto ip sla mpls reset** command.

- CSCsu33399

  Symptoms: HWIC-4SHDSL:4Wire annex F/G with coding 16/32 TCPAM link on central office (CO) side is going down.

  Conditions: 4-WIRE SHDSL card with F/G annex-coding 16/32 TCPAM link on CO side is going down. CO link goes down immediately when either F/G annex is configured and never comes up. But the link on the CPE side will come up.

  This Issue is seen with F/G annex; the issue is not seen with A/B annex. The CO side link goes down, but the CPE comes up.

  Workaround: There is no workaround.

- CSCsu35963

  Symptoms: IPIPGW/CUBE will not respond to a H.245 emptyCapabilitySet, for example, TerminalCapabilitySet(TCS)=0 message from Cisco Voice Portal (CVP) with a CloseLogicalChannel(CLC) message. This will result in call failure.

  Conditions: This symptom occurs when IPIPGW is deployed in H.323-H.323 mode that is running Cisco IOS Release 12.4(20)T and interacting with Cisco Voice Portal (CVP).

  Workaround: There is no workaround.

- CSCsu36827

  Symptoms: The CUE clock does not synch up with the CME using NTP.

  Conditions: This symptom is observed when the UC500 is configured as the NTP master.

  Workaround: Use an external NTP server other than the UC500.

- CSCsu36836

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

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

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

- CSCsu40234

  Symptoms: When GetVPN and time-based anti-replay are configured with the VSA module, no packets will pass through the router.

  Workaround: Remove time based anti-replay from the GetVPN Key Server configuration

- CSCsu45608

  Symptoms: A zone-based firewall does not allow returned TCP traffic from a VPN tunnel.

  Conditions: This symptom is observed when the firewall is configured to inspect TCP traffic to and from the VPN tunnel.

  Workaround: There is no workaround.

- CSCsu47027

  Symptoms: Device crashes 10-15 times per day when receiving calls from an end customer using an Asterisk PBX.

  Conditions: This symptom is observed in Cisco IOS Releases 12.4(21) and 12.4(20)T.

  Workaround: There is no workaround.

- CSCsu47037

  Symptoms: A router crashes when an attempt is made to forward a packet out of an Auto-Template interface. This occurs since the interface MTU is set to 0: “show interface Auto-Template X” shows an MTU of 0.

  Workaround: Configure a protocol MTU directly on the Auto-Template interface (e.g. ip mtu XXXX).

- CSCsu51095

  Symptoms: If connected routes are optimized using PfR, there will be a routing loop.

  Conditions: This symptom can occur if, for some reason, PfR is learning connected routes or if the user has configured them.

  Workaround: Create an oer-map with a prefix-list that contains the prefixes with the IP addresses of the connected routes (the next hops). Set the set observe mode in the oer-map.

- CSCsu51668

  Symptoms: Box crashes when reattaching the Map-class (or) access the time-slots in a controller mode.

  Conditions: This symptom is seen on a Cisco 7200 series router with HQF + FRF.12.

  Workaround: There is no workaround.

- CSCsu53032

  Symptoms: In rare cases a router will crash upon removing a trustpoint in global configuration mode.

  Conditions: This symptom is observed on some hardware platforms. Other platforms will handle this gracefully.

  Workaround: Reload the router and upgrade to a version with the fix.

- CSCsu54546

  Symptoms: When running EasyVPN client on a router, the EasyVPN connection will go down and then renegotiate whenever the ISAKMP lifetime expires.

  Workaround: There is no workaround. You can increase the ISAKMP lifetime to 86400 to minimize service interruptions.

- CSCsu58237

  Symptoms: A router crashes due to “TLB (load or instruction fetch) exception”.

  Conditions: This symptom may be encountered if the **upgrade automatic** command is executed to download an image from cisco.com. This bug affects Cisco IOS platforms which have “Auto Upgrade Manager” feature.

  Workaround: There is no workaround.

- CSCsu60252

  Symptoms: A Cisco router may unexpectedly reload due to a bus error exception or due to software forced crash due to SYS-3-BADFREEPTRS.

  Conditions: This symptom is observed when the router is running IPS.

  Workaround: Turn off IPS.

- CSCsu61665

  Symptoms: The router crashes on session establishment or termination over a VMI interface with “debug vmi pppoe” on.

Conditions: This symptom is observed when “debug vmi pppoe” is enabled, and a session must be being initiated or terminated.

Workaround: Disable “debug vmi pppoe”.

- CSCsu61741

  Symptoms: LSP ping CLI is missing.

  Conditions: This issue is specific to the Cisco 7301.

  Workaround: There is no workaround.

- CSCsu61953

  Symptoms: In 6VPE topology, IPv6 routes are not propagated properly to 6VPE router. Actually the IPv6 prefixes, although included in the update message, are being sent in an invalid format. On the receiving router, the decoded IPv6 prefix is a different entry from the actual prefix sent. The actual IPv6 prefix is lost and not propagated.

  Conditions: This symptom occurs only in 6VPE case with a nonconnected nexthop, and an IPv4 mapped IPv6 nexthop is to be sent. The nexthop field is not set properly.

  Workaround: There is no workaround.

  Further Problem Description: When the prefix label is compared with the wrong macro mentioned above, the gateway of the prefix or the nexthop was not set properly. The nexthop, instead of being set to an IPv4 mapped IPv6 address, is set to the global IPv6 nexthop. Since this is not a connected nexthop, the label allocation is not done. This prefix being via 6VPE when received on the other other end, the decoding of the message occurs as though the label exists. So the prefix retrieved from the message will be different from the actual prefix sent, which is the problem.

- CSCsu62921

  Symptoms: %SYS-2-BADSHARE tracebacks are reported. Eventually the router will stop passing all traffic over the interface.

  Conditions: This symptom occurs when sending traffic over xDSL interfaces that have QoS configured.

  Workaround: Remove the service-policy from the xDSL interface.

- CSCsu67369

  Symptoms: A Cisco 7200 router with a VSA may crash if it receives high inbound traffic when it is downloading large number of GETVPN SAs.

  Conditions: This symptom occurs when a Cisco 7200 router with a VSA receives high inbound traffic when it is downloading large number of GETVPN SAs.

  Workaround: There is no workaround.

- CSCsu68245

  Symptoms: A router crashes.

  Conditions: This symptom occurs when the traffic is flowing and if the interface is **shut** followed by **no shut**.

  Workaround: There is no workaround.

- CSCsu78451

  Symptoms: The CLI “webvpn create template” shows svc-translation-table as one of the options on giving “?” on the CLI.

  Conditions: This symptom affects releases on Cisco IOS Release12.4(22)T.

Workaround: No side effect, it is a CLI which should be hidden.

Further Problem Description: Svc-translation-table option is not supported. It should be hidden.

- CSCsu87180

  Symptoms: The MPLS support/CLI is missing in Cisco 3270 released images in Cisco IOS Release 12.4(15)T.

  Conditions: The support was deprecated in Cisco IOS interim Release 12.4(18.04)T1 and Release 12.4(15)T3.

  Workaround: There is no workaround.

- CSCsu88745

  Symptoms: SCCP phones fail to register with Cisco Unified CallManager Express (CME).

  Conditions: This symptom occurs when auto register is enabled without ephone/ephone-dn configuration.

  Workaround: Configure ephone and ephone-dn for all SCCP phones.

Resolved Caveats—Cisco IOS Release 12.4(20)T6

Cisco IOS Release 12.4(20)T6 is a rebuild release for Cisco IOS Release 12.4(20)T. The caveats in this section are resolved in Cisco IOS Release 12.4(20)T6 but may be open in previous Cisco IOS releases.

- CSCsu47486

  Symptoms: Cisco IOS Software configured with MGCP may reload.

  Conditions: This symptom is observed if an authenticated user repeatedly configures **mgcp block-newcall**, **no mgcp block-newcall** while active calls are being made.

  Workaround: Wait for all active calls to terminate before configuring **no mgcp block-newcall**.

- CSCsw40203

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

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

  Workaround: There is no workaround.

- CSCsy29533

  Symptoms: A T.38 fax relay call may fail.

  Conditions: The symptom is observed with an MGCP-controlled T.38 fax relay call when the gateway is configured for CA control T.38. The output of the **debug voip vtsp all** command shows fax relay as “DISABLED.”

  Workaround: Use Cisco IOS Release 12.4(15)T7 or Release 12.4(22)T.

- CSCsz43987

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

  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://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.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://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCsz45539

  Symptoms: Unable to attach the frame relay DLCI to the serial subinterface. The following error is received:

  ```
  %PVC already assigned to interface Serial3/0
  ```

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

  Workaround: There is no workaround.

- CSCta07104

  Symptoms: The **mpls bgp forwarding** command is not synced to the standby router.

  Conditions: When the **mpls bgp forwarding** command is not configured manually on the ASBR router, when eBGP Inter-AS session comes up, the command is auto-generated on the interface. The command is not synced to the standby router.

  Workaround: The issue will not be seen:

  1. When the **mpls bgp forwarding** command is configured manually.
  2. When the command is not configured manually, after a switchover, both the active router and the standby router will get that command.

- CSCta62678

  Symptoms: A router hangs when an access-control service policy is reconfigured.

  Conditions: This symptom is observed on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCta85026

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

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

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

Workaround: There is no workaround.

- CSCtb18207

  Symptoms: A router crashes.

  Conditions: The symptom is observed when configuring IPSec using the VTI and attaching the service policy to the tunnel interface, while enabling the physical interface and where the tunnel source in the tunnel interface is given as IP address of the physical interface. It is observed when the router is loaded with the c7200-adventerprisek9-mz.124-24.6.PI11r image.

  Workaround: Use the physical interface instead of using the VTI for IPSec.

- 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.

- 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.

- CSCtb73450

  Symptoms: Start-Control-Connection-Request (SCCRQ) packets may cause tunnel to reset after digest failure.

  Conditions: This symptom is observed when the SCCRQ packets are sent with an incorrect hash.

  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://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.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://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

- 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.

- CSCtd33567

  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://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.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://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  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

- CSCtd62885

  Symptoms: IKE renegotiation might fail for minutes while one peer displays:

  ```
  %CRYPTO-6-IKMP_NOT_ENCRYPTED: IKE packet from <ip> was not encrypted and it should've been
  ```

  Conditions: The symptom is observed when certificates are used. The signature verification might fail after MM5 or MM6 messages are exchanged preventing the tunnel establishment. The issue seems to hit Cisco IOS Release 12.4(20) T3 and Release 12.4(24)T2. It affects only Cisco 7200 series routers with VSA modules.

  Workaround: Use pre-shared keys.

- 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://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.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://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

- 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.

- 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.

- 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.

- CSCtf17624

  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://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.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://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  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

- CSCtf72678

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

  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://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.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://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  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

  Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

  http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

  http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a313.shtml

- CSCtf87559

  Symptoms: HWIC-4ESW drops some of the multicast packets while transmitting due to output errors.

  Conditions: This symptom is observed when multicast packets are received on an onboard FE port and transmitted via the HWIC-4ESW to the LAN using a VLAN interface. As the multicast traffic rate increases, the drop rate of the HWIC- 4ESW increases. Show controller for the HWIC-4ESW port shows "MAC IDB Tx Errors: output_drops" incrementing. The issue is not seen with unicast traffic.

  Workaround: There is no workaround.

- CSCtf91428

  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://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.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://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

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

- 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.

- CSCtg21685

  Cisco IOS Software contains a vulnerability when the Cisco IOS SSL VPN feature is configured with an HTTP redirect. Exploitation could allow a remote, unauthenticated user to cause a memory leak on the affected devices, that could result in a memory exhaustion condition that may cause device reloads, the inability to service new TCP connections, and other denial of service (DoS) conditions.

  Cisco has released free software updates that address this vulnerability. There is a workaround to mitigate this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-sslvpn.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://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  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

- 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.

- 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.

- 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 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.

- 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.

Resolved Caveats—Cisco IOS Release 12.4(20)T5

Cisco IOS Release 12.4(20)T5 is a rebuild release for Cisco IOS Release 12.4(20)T. The caveats in this section are resolved in Cisco IOS Release 12.4(20)T5 but may be open in previous Cisco IOS releases.

- 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.

- CSCsq99299

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

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

  Workaround: There is no workaround.

- CSCsu05306

  Symptoms: A Cisco device might report a crash because of a software-forced crash and/or bus error. The root cause for the crash: refcount becomes -1 as the chunk was already freed.

  Conditions: This symptom is observed on a Cisco device only when an application firewall for HTTP inspection is turned on.

  Workaround: There is no workaround.

- CSCsu78975

  Symptoms: A crash is seen at adj_switch_ipv4_generic_les on a Cisco 38xx router.

  Conditions: This symptom is observed upon issuing the **no ip route 10.2.82.0 255.255.255.0 vlan1** command.

  Workaround: There is no workaround.

- CSCsv62323

  Symptoms: The Fast Ethernet driver code may cause several errors. The observed symptoms of this issue include:

  - Cisco Unified Communications 500 series routers (UC520) may crash with an "Unexpected exception to CPU" error.
  - A Cisco 1861 router may fail to establish an L2TPv3 session with an error message:

```
%L2TP-3-ILLEGAL: _____:________: ERROR: unsupported transport protocol; defaulting
to UDP if possible
```

  Conditions: The symptoms are observed with the following hardware platforms: UC520, Cisco 880 series, Cisco VG202, Cisco VG204, IAD2435-8FXS, and Cisco 1861 routers. In addition, the following conditions exist:

  - The UC520 must be configured with a BVI interface. For example:

```
interface BVI1
 ip address 192.168.0.1 255.255.255.0
```

  - The Cisco 1861 router is configured with L2TPv3. For example:

```
pseudowire-class l2tpv3
 encapsulation l2tpv3
 ip local interface Loopback0
!
interface Loopback0
 ip address 192.168.10.1 255.255.255.255
!
interface FastEthernet0
 no ip address
 xconnect 192.168.0.1 1 pw-class l2tpv3
```

  Workaround: There is no workaround.

  Further Problem Description: The issue is caused by an underlying driver vulnerability that exists in the UC520, Cisco 880 series, Cisco VG202, Cisco VG204, IAD2435-8FXS, and Cisco 1861 routers. No other models of Cisco routers/switches are known to be affected by this issue. The symptoms can be triggered with specific TCP sequences.

- CSCsx26025

  Symptoms: Wireless clients are not able to ping each other after a few minutes.

  Conditions: This symptom can occur on any of the following routers with 802.11 wireless interfaces:

  - UC500
  - 85x
  - 87x
  - 1811
  - HWIC-AP

  Workaround: There is no workaround.

- CSCsy61321

  Symptoms: Accounting requests keep on sending to TAC server, which is failing.

  Conditions: This problem will happen when we configure authentication as none and accounting with TACACS.

```
!
aaa authentication login default none
aaa accounting exec default start-stop group one group two
!
```

The criteria are as follows:

The group one server should be reachable, and the TAC daemon should not run on the server. The group two server is perfect.

Workaround: Works fine with a single working server or when the first group has a valid server.

- CSCsy74023

  Symptoms: A slow memory leak occurs, mainly in the 72 bytes, 80 bytes, and possibly 192 bytes memory region blocks.

  Conditions: This symptom is observed with a large number of IPSec peers (more than 100) and several thousand tunnels when Phase I is authenticated by RSA-SIG.

  Workaround: There is no workaround.

- CSCsz05181

  Symptoms: A router may reload unexpectedly.

  Conditions: The symptom is observed when the router has Bidirectional Forwarding Detection (BFD) configured and is actively sending keepalives. The crash has multiple possible triggers:

  – It can be triggered by certain **show** commands (the **show bootvar** and **show c7200** commands are known to cause the problem). The issue will not be seen on every invocation of the commands. It is a rare timing condition, so the probability of the crash increases as the commands are run more frequently.

  – It can also be triggered by large-scale BFD deployments (hundreds of sessions on a single router).

  Workaround: Unconfigure BFD.

- CSCsz14273

  Symptoms: A Cisco IOS device may produce CPUHOG error messages and a watchdog timeout unexpected restart when running a Tool Command Language (Tcl) Embedded Event Manager (EEM) policy.

  Conditions: This occurs when the EEM policy uses the Tcl **puts** command to print a very large amount of text.

  Workaround: Do not use this command to print a large amount of text.

- CSCsz48614

  Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCsz50423

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

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

  Workaround: There is no workaround.

- CSCsz56382

  Symptoms: The Tunnel0 interface that is used on a DMVPN hub is reporting “Tunnel0 is reset, line protocol is down” or no traffic is passing through this interface anymore.

  The IKE and IPSec SAs may still be up, but only the decaps counters will be seen increasing, not the encaps counters.

  Conditions: This symptom is observed on Cisco 2821 routers that are running Cisco IOS Releases 12.4(9)T7 or 12.4(15)T9. Other platforms and releases may be affected.

  Workaround: Shut down Tunnel0 and, instead, create interface Tunnel1 with the same configuration, if you cannot reload the router.

  Otherwise reloading the router will resolve the issue. Do not configure another identical Tunnel interface in this case or you will run into CSCsl87438. If you reload the router at a later time, be sure to remove the duplicate Tunnel interface prior to the reboot.

- CSCsz72138

  Symptoms: A POS interface on a PA-POS-2OC3 may experience a stuck issue. All packets will be dropped after hitting the stuck scenario:

  ```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
  72048413<<<<<<<<<<<<<<<<<<<<all packets are getting dropped Queueing strategy:
  Class-based queueing Output queue: 197/1000/0 (size/max total/drops)<<<<<<<<<<output
  queue remains stuck at 197
  ```

  Conditions: This issue is common to different platforms such as the Cisco 7300, Cisco 7304, and Cisco 7200. Stuck can happen with and without service policy also.

  Workaround:

  1. Do a shut/no shut of the affected interface.

  2. Do a soft OIR of the affected slot.

- CSCsz72591

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

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

  Workaround: There is no workaround.

- CSCta05809

  Symptoms: A group member on a GETVPN network may stop passing encrypted traffic.

  Conditions: A GETVPN group member (GM) may accept and process an old or duplicate rekey message from the designated key server (KS). If the rekey message includes a TEK that was previously used to encrypt data but that has already expired, the GM may become unable to send and receive encrypted traffic.

  Workaround: There is no workaround.

- CSCta09049

  Symptoms: Memory leak chunk in alloc-proc “encrypt proc” or “Pool Manager” of name “Packet Header” is observed.

  Conditions: The device is being used as a crypto endpoint.

  Workaround: There is no workaround.

  Further Description: pak_with_particles_duplicate()

In this function we get a new pak from the same pak pool as the original pak, which in our case is most of the times the fs_pakpool. The fs_pakpool however has the property to not put the pak back in the pool when datagram_done() is called. Therefore we end up leaking paks.

- CSCta10075

  Symptoms: An incorrect logic in doing increment comparisons for counters, such as interface resets, will cause an EEM policy to be triggered. That is, if there are any numbers in the interface resets counter and a **clear counters** command is performed, on the next EEM poll interval, the command executes, which is not correct.

  Conditions: This symptom is observed in the latest Cisco IOS Release 12.4(24)T. Most of the newer 12.4T images are also affected.

  Workaround: There is no workaround.

- CSCta16724

  Symptoms: Users with level 15 privilege and a “view” cannot do a Secure Copy (SCP).

  Conditions: This symptom is observed when a user with a “view” attempts to do an SCP.

  Workaround: Remove view.

- 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.

- CSCta24037

  Symptoms: A Cisco router may reload due to a bus error and display the following messages:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 10:09:03 PDT Tue Sep 1 2009 addr=0x0,
  pc=0x4159DB10z , ra=0xFFFFB4DFz , sp=0x4F059900
  %ALIGN-1-FATAL: Illegal access to a low address 10:09:03 PDT Tue Sep 1 2009 addr=0x0,
  pc=0x4159DB10z , ra=0xFFFFB4DFz , sp=0x4F059900
  TLB (store) exception, CPU signal 10, PC = 0x415A2630
  ```

  Conditions: This symptom is observed on a Cisco 2851 router that is running Cisco IOS Release 12.4(24)T1.

  Workaround: There is no workaround.

- CSCta32825

  Symptoms: A Cisco router may crash with a bus error after a class map is configured or a class map is modified.

  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 symptom has been seen only while traffic is trying to match against the policy while it is being updated.

- CSCta45976

  Symptoms: A BFD session cannot be established to the peer if the same IP address is configured on the device in a different VRF.

  Conditions: The symptom is observed when BFD sessions stay in a down state.

  Workaround: Remove the locally configured IP address.

- CSCta49840

  Symptoms: GGSN may encounter a fatal error in VPDN/L2TP configurations.

  Conditions: The symptom is observed in rare race conditions when physical connectivity on the interface to LNS is lost while there are active sessions and traffic.

  Workaround: There is no workaround.

- CSCta66499

  Symptoms: The Cisco IOS MGCP gateway may experience a software-forced reload.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(20)T4 or a later release when re-enabling MGCP with version 1.0 after testing fgdos calls with MGCP version 0.1.

  Workaround: There is no workaround.

- CSCta77678

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

- CSCta86675

  Symptom: A Cisco router may crash reporting a bus error.

  Conditions: Stress traffic is being passed through a Cisco router that is configured with QoS policies, a crypto map, and access lists.

  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.

- CSCtb13546

  Symptoms: A Cisco IOS router crashes with a bus error.

  Conditions: This symptom occurs when a Cisco IOS router is performing multihop VPDN (also known as tunnel switching). The router may crash infrequently due to a bus error.

  This crash is limited to cases where at least one of the following VPDN group commands are configured:

  - **ip pmtu**
  - **ip tos reflect**

  Workaround: Disable the above mentioned commands. However, the consequences of this on user traffic must be evaluated first.

- 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.

- CSCtb29256

  Symptoms: A router crashes after the **sh isdn history** command is entered.

  Conditions: This issue is seen in a Cisco 7206VXR (NPE-G2) that is running Cisco IOS Release 12.4(15)T9.

  Workaround: Avoid using the **sh isdn history** command; use the **sh isdn active** command instead.

- 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.

- CSCtb57180

  Symptoms: A router may crash with a software-forced crash.

  Conditions: Under certain conditions, multiple parallel executions of the **show users** command will cause the device to reload.

  Workaround: It is possible to limit the exposure of the Cisco device by applying a VTY access class to permit only known, trusted devices to connect to the device via telnet, reverse telnet, and SSH.

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

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

  The following example permits access to VTYs from the 192.168.1.0/24 netblock and the single IP address 172.16.1.2 while denying access from everywhere else:

  ```
  Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
  Router(config)# access-list 1 permit host 172.16.1.2
  Router(config)# line vty 0 4
  Router(config-line)# access-class 1 in
  ```

  For devices that act as a terminal server, to apply the access class to reverse telnet ports, the access list must be configured for the aux port and terminal lines as well:

```
Router(config)# line 1 <x>
Router(config-line)# access-class 1 in
```

Different Cisco platforms support different numbers of terminal lines. Check your device's configuration to determine the correct number of terminal lines for your platform.

Setting the access list for VTY access can help reduce the occurrences of the issue, but it cannot completely avoid the stale VTY access issue. Besides applying the access list, the following is also suggested:

1. Avoid nested VTY access. For example, RouterA->RouterB->RouterA->RouterB.

2. Avoid issuing the **clear vty** command or the **clear line** command when there is any nested VTY access.

3. Avoid issuing the **clear vty** command or the **clear line** command when there are multiple VTY accesses from the same host.

4. Avoid issuing the **clear vty** command or the **clear line** command when router CPU utilization is high.

5. Avoid issuing the **show users** command repetitively in a short period of time.

Again, the above can help reduce the occurrences of the issue, but it cannot completely avoid the issue.

- 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: This symptom is observed with Cisco IOS Release 12.4(24)T1.

  Workaround: There is no workaround.

- CSCtb60330

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

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

  Workaround: Disable DPDs.

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

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

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

  The following entry can be seen in debugs:

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

- 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 the **show run | format** *x* command if there is a general route map configured in the router.

- 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.”

- 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.

- 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.

- 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.

- CSCtc01912

  Symptoms: Consider the following **debug isdn q931** snippet and partial Embedded Event Manager (EEM) script:

  ```
  Router# 000023: *May 29 23:00:35.600 EST: ISDN Se1/0:23 Q931: RX <- SETUP pd = 8
  callref = 0x614B Bearer Capability i = 0x8090A2 Standard = CCITT <SNIP>
  !
  event manager applet ISDNtrap
  event syslog occurs 1 pattern ".*Bearer Capability.*"
  action 1.00 syslog msg "ISDN Message Observed!"
  ```

```
action 1.01 syslog msg "Starting GW status snapshot data collection."
<more stuff>
!
```

In Cisco IOS Release 12.4(20)T, it turns out that the EEM script will trigger on debug text on the first line of the output, say "RX <- SETUP," but it will not trigger on text in the body of the message like "Bearer Capability."

Conditions: This behavior is observed on Cisco IOS routers that are configured with an EEM script that triggers based on the instance of a specified text string in a **debug** message appearing in the logging buffer. Only Cisco IOS Release 12.4(20)T is affected.

Workaround: Use an unaffected Cisco IOS 12.4T release such as 12.4(15)T, 12.4(22)T, and 12.4(24)T.

- CSCtc12312

  Symptoms: PKI might get stuck after 32,678 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.

- 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.

- 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.

- 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.

- 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.

- CSCte10706

  Symptoms: When you configure FRF.12 “frame-relay fragment 512 end-to-end” on the serial interface, the router crashes.

  Conditions: The symptom is observed when you configure FRF.12 “frame-relay fragment 512 end-to-end” on a CJ-PA.

  Workaround: There is no workaround.

- 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://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  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 that is running Cisco IOS Release 12.4(24)T2 is connected to a third-party DSLAM that is 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 “clear pppoe all”:

```
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
```

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 running the following Cisco IOS releases:
   - 12.4(15)T7
   - 12.4(15)T10
   - 12.4(20)T
   - 12.4(22)T
   - 12.4(22)T1
   - 12.4(24)T
   - 12.4(24)T1
   - 12.4(24)T2
   - 15.0(1)M
3. The symptom can be triggered three ways:
   - 3A. “reload”
   - 3B. If “reload” results in correct behavior, “clear pppoe all.”
   - 3C. If “reload” results in correct behavior, any subsequent event that results in both PPPoE sessions being torn down simultaneously.
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, and then follow Workaround 1.

- 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.

- 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.

Resolved Caveats—Cisco IOS Release 12.4(20)T4

Cisco IOS Release 12.4(20)T4 is a rebuild release for Cisco IOS Release 12.4(20)T. The caveats in this section are resolved in Cisco IOS Release 12.4(20)T4 but may be open in previous Cisco IOS releases.

- CSCsd77560

  Symptoms: SNMPv3 “auth” and “priv” users are lost across reload.

  Conditions: Occurs after a reload.

  Workaround: There is no workaround.

- CSCsg00102

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

  Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed.

  This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix CSCso04657 and CSCsg00102.

- CSCsj17977

  Symptoms: The GETVPN rekey fails. The following error message shows in the syslog:

  %GDOI-3-GM_NO_IPSEC_FLOWS: IPSec FLOW limit possibly reached

  The **show crypto engine connections flow** will show that all flows are used. For hardware-accelerated platforms, use the **show crypto eli** command to see how many Phase IIs are supported.

  Conditions: This problem is seen when the registration is not successful on a group member and then the flow IDs allocated for that incomplete registration are not cleaned up.

  Workaround: Reload the router, if the all the flow IDs are leaked.

- CSCsk80396

  Symptoms: Router crashes when jitter operation takes place.

  Conditions: This crash is inconsistent and is seen while auto Ethernet operation is configured to carry on jitter operation on an interface configured with **no ethernet cfm enable**.

  Workaround: There is no workaround.

- CSCsl15443

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

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

  Workaround: There is no workaround.

- CSCso53496

  Symptoms: When using Group Encrypted Transport VPN (GET VPN) feature, the df-bit override (on IPSec packets) feature is not working. This means that **crypto ipsec df-bit set|clear** commands have no effect, both on a global or per-interface basis.

  Conditions: The bug is only seen when GETVPN is used. Legacy IPSec tunnels are not affected.

  Workaround: There is no workaround.

- CSCsq58289

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

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

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

- CSCsr16147

  Symptoms: Session is not getting disconnected when the locally configured timers expire.

  Conditions: Occurs while testing an internal build of Cisco IOS Release 12.4(22)T on the Cisco 7200.

  Workaround: There is no workaround.

- CSCsr60092

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

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

  Workaround: There is no workaround.

- CSCsr62645

  Symptoms: Software-forced reload occurs on Cisco 870 router.

  Conditions: Encountered during extended VLAN testing.

  Workaround: There is no workaround.

- CSCsr83201

  Symptoms: A Cisco AS5350XM or AS5400XM may reload with a message similar to:

  ```
  *Jun 16 08:02:05.951: %CRYPTO-0-SELF_TEST_FAILURE: Encryption self-test failed (RSA
  Signature)
  ```

  The device may be unable to generate RSA keypairs:

  ```
  ssh-server(config)#crypto key generate rsa
  The name for the keys will be: ssh-server.cisco.com
  Choose the size of the key modulus in the range of 360 to 2048 for your General
  Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
  How many bits in the modulus [512]: 1024
  % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
  % Error in generating keys: could not generate test signature
  crypto_lib_keypair_get failed to get ssh-server.cisco.com
  crypto_lib_keypair_get failed to get ssh-server.cisco.com
  ```

  Conditions: Occurs when running Cisco IOS Release 12.4(20)T or 12.4(15)XY2.

  Workaround: Load a non-crypto image.

- CSCsr83550

  Symptoms: An SRTP call may fail through a Cisco Multiservice IP-to-IP Gateway (IPIPGW).

  Conditions: The symptom is observed when a secure SRTP call is made between two CCMs with an IPIPGW in between.

  Workaround: There is no workaround.

- CSCsr88705

  Symptoms: Redistributed routes are not being advertised after a neighbor flap.

  Conditions: This symptom is observed if BGP is redistributing local routes and if there are multiple neighbors in the same update-group and then a neighbor flaps. For the flapped neighbor, some redistributed routes are not being advertised.

  Workaround: Undo and redo the redistribution.

- CSCsr90248

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

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

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

- CSCsr96084

  Symptoms: A router crashes with the following error:

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

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

  ```
  Workaround: Use PBR for locally-generated traffic to force the GRE packet out of the
  physical interface which prevents the lookup that can lead to the recursion. For
  example (note: the interfaces and IPs will need to be changed to the appropriate
  values):
  interface Tunnel97 ... tunnel source POS6/0 ...
  interface POS6/0 ip address 10.2.0.1 255.255.255.252
  ip local policy route-map Force-GRE
  ip access-list extended Force-GRE permit gre host 10.2.0.1 any
  route-map Force-GRE permit 10 match ip address Force-GRE set interface POS6/0
  ```

- CSCsu00313

  Symptoms: SRTP call fails through IP-IP gateway with SIP end points.

  Conditions: SRTP call may fail with SIP trunk in between two CUCMs that are connected through IP-IP gateway.

  Workaround: There is no workaround.

- CSCsu32452

  Symptoms: Spurious memory access occurs.

  Conditions: Occurs while attempting to unconfigure the EzVPN client configuration on an EzVPN client inbound interface.

  Workaround: There is no workaround.

- CSCsu50252

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsu58763

  Symptoms: Card crashed upon attaching the policy-map to the output interface.

  Conditions: Happening in all types of VCs (PVC/SVC) when the service policy is defined with **shape** command.

  Workaround: There is no workaround.

- CSCsv01931

  Symptoms: SSLVPN logins from test tool are unsuccessful. The **show crypto eng acc stat** command displays a large number of API request errors.

  Conditions: This happens when using the hardware crypto engine on a Cisco 1811 router.

  Workaround: Disable the hardware crypto engine and use the software crypto engine.

- CSCsv17698

  Symptoms: Packets may be incorrectly classified under child and parent classes.

  Conditions: The symptom is observed when a two or three-level policy is configured/reconfigured coupled with the command **clear counters**. The symptom also occurs if a second level policy-map is detached and then re-attached to a grandparent policy. Some of the packets go through the intended parent (or grandparent) class and incorrectly go through the default class or no class at all of the child policy.

  The issue is seen with a Cisco 7200 series router that is running Cisco IOS Release 12.4(20)T2, 12.4(22)T2 or 12.4(24)T.

  Workaround: Reload the router. In some cases, unconfiguring and reconfiguring the policies will work.

- CSCsv40340

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

  Conditions: This symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4(15)T7. The router is configured with NHRP.

  Workaround: There is no workaround.

- CSCsv48603

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsv55810

  Symptoms: A Cisco router may reload unexpectedly due to a software forced crash:

  ```
  001286: Nov 5 13:14:22: %SYS-6-STACKLOW: Stack for process AAA Per-User running low,
  0/6000
  %Software-forced reload
  ```

Conditions: This has been experienced on a Cisco 2811 router running Cisco IOS Release 12.4(20)T1 and 12.4(22)T. The router is configured with AAA.

Workaround: There is no workaround.

- CSCsv65867

  Symptoms: NM-CEM-4SER modules installed in Cisco 3845 routers will not use network clock if one is available. Instead, they will use the local oscillator. This can be observed by using the **show cem** *slot/port/0* command.

  Conditions: This behavior is observed on a NM-CEM-4SER module installed in Cisco 3845 routers running Cisco IOS Release 12.4(20)T or later.

  Workaround: Use adaptive clocking to improve clock accuracy.

- CSCsv91628

  Symptoms: BGP prefixes are not exchanged between route reflectors.

  Conditions: Occurs when route reflectors are present in different AS and they have MP-EBGP relationship between them.

  Workaround: There is no workaround.

- CSCsw18636

  Symptoms: High CPU utilization occurs after device receives a ARP packet with protocol type as 0x1000.

  Conditions: This problem occurs on Supervisor 32 running Cisco IOS Release 12.2(33)SXI. This problem may also occur on Supervisor 720. The problem is only seen when you have bridge-group CLI being used, which leads to ARP packets with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

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

- CSCsw23314

  Symptoms: A router reloads when a manually keyed crypto map is removed from an interface after unconfiguring the tunnel source.

  Conditions: The symptom is observed when the manually keyed crypto map is applied on the tunnel interface. The crash happens when the user cuts and pastes several “no” forms of the CLI in order to delete the tunnel source interface as well as removing the crypto from the tunnel and deleting the tunnel interface itself:

  ```
  conf t int tunnel0
  no ip addr x.x.x.x x.x.x.x
  no tunnel source e1/0
  no tunnel dest y.y.y.y
  no crypto map !
  must be a manually keyed crypto map
  exit
  no interface tunnel0
  ```

  The issue occurs only on a Cisco 7200 series router with VSA, a Cisco ASR 1000, or a Cisco Catalyst 6000 Series Switch with VPNSPA.

  Workaround: Enter the commands one at a time, waiting after removing the tunnel source. This will prevent the race condition from occurring, avoiding the crash.

- CSCsw65933

  Symptoms: The CE does not learn the prefix from one of the PEs.

  Conditions: The symptom is observed after configuring (on PE2):

```
router bgp 10 address-family ipv4 vrf test1 no neighbor <peer > route-map setsoo in
end
```

and then clearing using the following command: **clear ip bgp** *peer vrf test1* **soft out**.

Workaround: Use the command **clear ip bgp * soft** on the PE after SOO is applied.

Alternate Workaround: On the CE, the command **clear ip bgp * soft** should not be applied within one minute after applying SOO route map to CE on UUT.

- CSCsw67252

  Symptoms: When RTP-NTE and T.38 are both enabled, the re-invite for T.38 incorrectly includes Session Description Protocol (SDP) with RTP-NTE.

  Conditions: Occurs when both RTP-NTE and T.38 are enabled.

  Workaround: There is no workaround.

- CSCsw80640

  Symptoms: A Cisco router may experience the following errors:

  ```
  %SYS-2-SHARED: Attempt to return buffer with sharecount 0, ptr= 659594E0 -Process= "IP
  Input", ipl= 4, pid= 93, -Traceback= 0x60C6C978 0x60373164 0x61556FC8 0x61558534
  0x612D6A44 0x612D8368 0x612D8780 0x612D883C 0x612D8A84 %SYS-2-SHARED: Attempt to
  return buffer with sharecount 0, ptr= 6649466C -Process= "IP Input", ipl= 4, pid= 93,
  -Traceback= 0x60C6C978 0x60373164 0x61556FC8 0x61558534 0x612D6A44 0x612D8368
  0x612D8780 0x612D883C 0x612D8A84
  ```

  Conditions: This symptom is observed on a Cisco 2801 router that is running Cisco IOS Release 12.4(20)T. The errors appear to be triggered with the forwarding of UDP packets.

  Workaround: There is no workaround. The problem does not appear to be service impacting.

- CSCsw85293

  Symptoms: The following CPUHOG messages are seen for Crypto ACL process:

  %SYS-3-CPUHOG: Task is running for (xxxx)msecs, more than (2000)msecs (9/7),process = Crypto ACL.

  Conditions: This has been seen on Cisco routers that are running Cisco IOS Release 12.4(15)T8 (other versions may be affected as well) with GETVPN configured.

  Workaround: Reducing the size and complexity of the crypto ACLs will often stop these errors.

- CSCsx08292

  Symptoms: When Service Policy is applied under the PVC, traffic flow across that interface stops.

  Conditions: The ping failure starts only after service-policy configuration.

  Workaround: There is no workaround.

- CSCsx20984

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

  Conditions: Unknown at this time.

  Workaround: There is no workaround.

- CSCsx29278

  Symptoms: Traceback will be seen if high amount of HTTP sessions are sent with Java blocking enabled.

  Conditions: Occurs on Cisco 3845 and Cisco 7200G1 routers with high number of HTTP connection per second and with HTTP inspection with Java blocking enabled. May occur on other platforms.

Workaround: Does not impact router functionality. The issue can be avoided by not enabling Java blocking.

- CSCsx32283

  Symptoms: Router is crashes.

  Conditions: Occurs because of malformed LDAP packet.

  Workaround: There is no workaround.

- CSCsx36091

  Symptoms: The input-queue size keeps increasing on the router until it hits the default value, after which packets are dropped at the interface.

  Conditions: Occurs with the following topology:

  IP phones ---- remote-site ---- WAN ---- central-site --- HQ ---- CUCM --- IP phones

  This is a single-NAT scenario, where the remote-site has all Application Level Gateway (ALG) enabled. Ten phones using Skinny Call Control Protocol (SCCP) on the remote site are trying to register to the Call Manager. Performing a **shut/no shut** on the WAN interface of the remote router triggers this scenario faster.

  Workaround: There is no workaround. Rebooting the router clears the queue.

- CSCsx42261

  Symptoms: Memory leak occurs with “CCSIP_SPI_CONTROL” process.

  Conditions: The error is found on a Cisco 3825 running the c3845-spservicesk9-mz.124-20.T1.bin image and using Skinny Call Control Protocol.

  Workaround: There is no workaround. Reload the router.

- CSCsx46421

  Symptoms: The file transfer aborts with the Active FTP.

  Conditions: The symptom is observed with the image c7200-adventerprisek9-mz.124-23.15.T3.

  Workaround: Use Passive FTP (**ip ftp passive**) for the FTP file to be properly transferred.

- CSCsx47227

  Symptoms: Incoming traffic on a PBR-configured interface is process switched.

  Conditions: The symptom is observed when traffic ingressing on an interface configured for PBR when using an ipbase, ipvoice, or entbase Cisco IOS images.

  Workaround: Disable PBR on the incoming interface.

- CSCsx51355

  Symptoms: Cisco 3845 used as a WAN aggregator will randomly crash when Frame Relay fragmentation is configured and with high traffic.

  Conditions: Occurs when branch routers are configured with FR, EIGRP, GRE, QOS, and Multicast. Traffic is sent. Occurs in an internal build of Cisco IOS Release 12.4(24)T.

  This crash would only happen when:

  1. Frame-relay is configured together with the QoS policy, and packet size is larger than the fragment size.
  2. Traffic exceeds 50% of line rate.

  Workaround: Remove the FR fragmentation configuration.

- CSCsx55861

  Symptoms: On a Cisco 880 router, the UUT crashes when the PVC comes up and when “auto qos voip” is configured.

  Conditions: The symptom is observed when “auto qos voip” is configured under ATM and when the PVC is toggled (due to, for example, a shut/no shut of the ATM interface or a cable being pulled and then restored).

  Workaround: There is no workaround.

- CSCsx56837

  Symptoms: Intermittent one-way audio occurs during a call.

  Conditions: Calls through a Cisco IOS transcoding device may experience one-way audio when certain signaling RTP payload types are received.

  Cisco IOS VoIP gateways utilize named signaling events (NSE) to signal certain transitions to other states for active calls. Modem passthrough is a feature by which two gateways can upspeed to g711 an active RTP session. This is signaled through the use of certain NSE packets between these devices.

  Modem passthrough using NSE through a transcoding session is not supported. However, under some situations on a voice call (no modems on the call), it is possible that the modem detection algorithm on the DSP may falsely detect a modem signal. If this occurs, a NSE will be sent out if modem passthrough is configured on the VoIP gateway. If the transcoder session that is bridging the two calls between the VoIP gateways receives this NSE packet, all further processing of RTP packets will stop in that direction.

  Workaround: Disable modem passthrough on the end VoIP gateways.

- CSCsx67255

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

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

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

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

  Workaround:

  1. Reload the router to clear the channel. If a reload cannot be done, busy out the channel with the failed calls using the **isdn busy b_channel** command under the serial interface.
  2. If this issue is due to oversubscription of the DSP resources, change the configuration to meet the DSP resources available on the gateway. Further information can be found with the CCO “DSP Calculator” at http://www.cisco.com/web/applicat/dsprecal/dsp_calc.html.
  3. If the issue is related to timing issues upon reload, shutdown the voice-port in question before reloading the gateway. When the gateway comes back up, take the voice-port out of shutdown.

- CSCsx68596

  Symptoms: The system may display a %SYS-3-NOELEMENT message, similar to:

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

  after which system behavior can be unpredictable. If the interrupts are rapid enough, the system may become unresponsive (hang), use all available memory to create more buffer elements, or crash due to CSCsj60426.

  Conditions: The message is caused by extremely rapid changes in flow control or modem control lead status on a console port.

  Workaround: Eliminate the source of the rapid lead changes. As modem control and flow control are generally not supported on the console, these changes are usually due to misconfigured devices attached to the console.

- CSCsx68730

  Symptoms: Pseudowire switching configured between ASBR routers does not work and tracebacks are seen.

  Conditions: Occurs when Cisco 7200 router is used as Autonomous System Border Router (ASBR) and pseudowire switching is configured.

  Workaround: There is no workaround.

- CSCsx70889

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsx75353

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

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

  Workaround: Remove the AIM compression card from the motherboard.

- CSCsx94324

  Symptoms: Packets with certain packet sizes get dropped when being CEF-switched on a router.

  Conditions: The symptom is observed when CEF is enabled and when the outbound interface is an HWIC-4SHDSL DSL interface. It is observed when the packet undergoes fragmentation.

  Workaround: Disabling CEF is a workaround.

- CSCsx95906

  Symptoms: Call fails when Nortel endpoint is at remote end.

  Conditions: Nortel endpoint sends a long contact header field value, which exceeds the maximum limit of the Cisco device. This remote contact overwrites memory for the from header and results in a dialog mismatch from the new message generated by the gateway.

  Workaround: There is no workaround.

- CSCsx98284

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

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

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

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

Alternate workaround: Separate the MTP functionality from the gateway.

- CSCsy05111

  Symptoms: A router crashes after enabling and disabling NBAR on an interface if a class-map with match protocol is configured first (“match protocol rtp audio”).

  Conditions: The symptom is observed if the “match protocol rtp audio” statement is found in the class-map configuration. RTP uses a label heuristic which quickly reproduces the bug.

  Workaround: Do a config/no-config on one interface while keeping NBAR configured on any other interface.

- CSCsy05298

  Symptoms: The IOSD-crash is seen and is affecting the main functionality.

  Conditions: This symptom is observed when a large number of groups (i.e. 50) is configured. The IOSD-crash is seen when we give the **show crypto gdoi** command after applying the general configuration and after checking the ping between all the PIM neighbors.

  Workaround: Use the **show crypto gdoi group** *group- name* to display a specific group’s information.

- CSCsy06128

  Symptoms: When a router is about to renew a certificate, the following syslog message is seen

  ```
  "%PKI-6-CERTRENEWAUTO: Renewing the router certificate for trustpoint xxx".
  ```

  However, no certificate is received until a few hours later.

  Conditions: The issue only happens on a Cisco 871 running Cisco IOS Release 12.4(15)T8 and 12.4(22)T1 or earlier releases. This issue is only seen with a very short certificate lifetime, such as 1 hour.

  Workaround: Increase the certificate lifetime to a few days or more.

- CSCsy07369

  Symptoms: An invalid range of IP addresses are accepted at CLI.

  Conditions: The symptom is observed when the following command format is used: **range** *ipaddress1 ipaddress2* where the range of the IP addresses is not seen in same network.

  Workaround: Avoid entering wrong ipaddress2.

- CSCsy09250

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

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

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

- CSCsy10893

  Symptoms: A router reloads occasionally after the command **show buffers leak** is repeatedly issued.

  Conditions: The symptom is observed when issuing 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.

- CSCsy16078

  Symptoms: A GETVPN group member might reload when removing “crypto map” from the interface, if that crypto map also contains a dynamic-map set together with the GDOI set.

  Conditions: The symptom only occurs when a dynamic-map set is added to a crypto map that is already applied to an interface and then the whole crypto map is removed, added and removed again. It is on the second removal that the reload occurs.

  Workaround: Execute the command **clear crypto gdoi** before removing the crypto map from the interface.

- CSCsy16177

  Symptoms: Cisco 2811 experiences invalid checksum over SCP on SSH version 2.

  Conditions: Occurs on a Cisco 2811 with flash type file system.

  Workaround: There is no workaround.

- CSCsy19659

  Symptoms: When using Point-to-Point Tunnelling Protocol (PPTP) with RADIUS Accounting, there may be several “nas-error” and “lost-carrier” listed in accounting as the Acct-Terminate-Cause.

  Conditions: The symptom is observed when using Cisco IOS Release 12.4T (Releases 12.4(15)T-12.4(22)T confirmed) and using PPTP with RADIUS Accounting in place.

  Workaround: There is no workaround.

- CSCsy20488

  Symptoms: IPSsec/GRE traffic does not go over an ATM interface.

  Conditions: The symptoms are observed when using a VSA encryption card and when the ATM interface is using PVC bundles.

  Workaround: Do not use PVC bundles.

  Alternate workaround: Disable the VSA encryption and use software encryption (not recommended for a high load of encryption).

- CSCsy22311

  Symptoms: Using secure copy (SCP) between Cisco routers may cause compatibility issues.

  Conditions: Occurs when using SCP SSH version 2 between a Cisco 1800 and Cisco 2800.

  Workaround: There is no workaround.

- CSCsy29940

  Symptoms: Unable to configure inspect for any protocol in self zone.

  Conditions: Occurs when configuring class-map with match protocol and trying to attach to self-zone pair.

  Workaround: The issue is not seen when **match access-group** is used.

- CSCsy31552

  Symptoms: A Cisco 1841 router equipped with xDSL WIC will suddenly stop forwarding packets. The packets will appear as output drops on the ATM interface statistics. Under the PVC level, there are no drops. The DSL line is not flapping but the ATM interface(s) report output drops.

  Conditions: The symptom is observed when using a Cisco 1800 and 2800 series router equipped with the same ADSL-WIC module. The ATM interface(s) need to be bridge-group configured. The bridge-group is in forwarding mode.

  Workaround: Reload the router.

- CSCsy32000

  Symptoms: Router crashes when BGP-IPv6 directly connected IBGP neighbors receives route with Link-local Nexthop.

  Conditions: BGP sends IPv6 link-local address in following cases:

  1. Directly connected eBGP neighbors
  2. BGP Ipv6 neighbors connected using Link-local address

  In case of this defect, testing device is advertising link-local nexthop for directly connected neighbor using global IPv6 address. Cisco router will never advertise link-Local nexthop.

  Workaround: There is no workaround.

- CSCsy32146

  Symptoms: Through-the-box traffic is dropped on the router (when the egress path is from the clear-text side to the encrypted side).

  Conditions: The symptom is observed with Cisco IOS Release 12.4(20)T and with L2TP over IPSec with a front door VRF.

  Workaround: Disable **ip route-cache** and **ip route-cache cef** on the clear-text interface (where the clear-text traffic comes from).

- CSCsy39667

  Symptoms: On a PPP aggregator using dhcp-proxy-client functionality, in a situation where a PPP client session is torn down and then renegotiated within 5 seconds, the DHCP proxy client may send a DHCP RELEASE for the previous DHCP handle after the new DHCP handle (created as a result of new IPCP CONFREQ Address 0.0.0.0) has accepted the same IP address allocation from the offnet DHCP Server. This results in the offnet DHCP server having no record of the lease as it exists on the PPP aggregator which causes future addressing conflicts.

  Conditions: The symptom is observed on a Cisco 7200 (NPE-400) and 7200 (NPE-G2) that is running Cisco IOS Release 12.4 T, or 12.2 SB.

  Workaround:

  1. Automated: Write a script to compare active leases on the PPP aggregator to active leases on DHCP server. If a lease is found to only exist on the PPP aggregator, use **clear interface virtual-access** to recover.
  2. Manual: use the command **clear interface virtual-access**.

  Further Problem Description: This issue occurs because the DHCP client holdtime is static at 5 seconds and there are no IOS hooks to tie PPP LCP session removal and IPAM to suppress stale DHCPRELEASES waiting in queue for HOLDTIME to expire.

- CSCsy40745

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

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

Workaround: Do not configure alternate SSH ports.

- CSCsy42401

  Symptoms: User group class matching fails when NAT is turned on.

  Conditions: The symptom is observed with IOS FW user group inter-operated with NAT.

  Workaround: There is no workaround.

- CSCsy43875

  Symptoms: A system may crash due to “Watchdog Time Expired” errors during normal operation without generating a crashinfo file or error messages prior to the crash.

  Conditions: The symptom is observed when any code tries to generate traceback via trace_caller. It is more likely to occur if BFD is configured.

  Workaround: There is no workaround.

- CSCsy45371

  Symptoms: The **clear ip nat tr *** command removes corresponding static NAT entries from the running configuration, but removing static NAT running configuration does not remove the corresponding NAT cache.

  Conditions: Occurs when NAT commands are entered while router is processing around 1 Mb/s NAT traffic.

  Workaround: Stop the network traffic while configuring NAT.

- CSCsy46007

  Symptoms: EzVPN tunnel will not come up after a reload. EzVPN is trying to connect to the peer with outside interface IP address to be “NULL”. The below debug message will be seen if “debug crypto isakmp” is enabled:

  ```
  EX: "ISAKMP:(0):receive null address from sa_req (local 0.0.0.0, remote 192.168.76.40)
  ```

  Conditions:

  1. EzVPN is in connect acl or auto mode
  2. Outside interface is configured on dialer interface.
  3. This issue is seen only when EzVPN is trying to ask the dialer to kick start and dialer is not yet ready or dialer has not yet assigned the IP address to the interface.

  Workaround: There is no workaround.

- CSCsy48838

  Symptoms: A router may crash with the following (or similar) message:

  %ALIGN-1-FATAL: Corrupted program counter

  Conditions: The symptom is observed when IOS firewall/ip inspect on H323 traffic is configured (“ip inspect name MY_INSPECT h323”).

  Workaround: Do not inspect H323.

- CSCsy52077

  Symptoms: Call passing through a Cisco Unified Border Element (CUBE) is dropped after more than 1 hour.

  Conditions: Occurs when there are multiple point-to-point calls going through CUBE at same time.

  Workaround: There is no workaround.

- CSCsy54122

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsy57750

  Symptoms: IPIPGW reloads while making an RSVP-enabled voice call with media statistics configuration.

  Conditions: The symptom is observed with Cisco IOS 12.4(24.6)T2 image.

  Workaround: There is no workaround.

- CSCsy58450

  Symptoms: Zone based firewall drops packets that pass through a VPN tunnel (both forward and reverse traffic). The drops are usually seen for UDP traffic. The following traceback may be seen:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (free) at interrupt level
  ```

  Conditions: Occurs when firewall is configured with crypto-map tunnels. Cisco IOS Release 12.4(20)T2 and 12.4(22)T and earlier releases are not affected.

  Workaround: Change the UDP timeout to a reasonably larger value. The default value is 30 seconds, and changing it to something like 300 seconds has been found to make a difference. To do this

  1. Create an “inspect” parameter map with any name if it does not exist, then add the new UDP idle timeout.

  parameter-map type inspect <param-map-name> udp idle-time 300

  2. Attach the parameter map to all the inspect actions. **policy-map type inspect <policy-name> class type inspect <class-name> inspect <param-map-name>**

- CSCsy69681

  Symptoms: Policy-based routing (PBR) fails to resolve next-hop.

  Conditions: Occurs when PBR is configured on a Cisco 871 to forward traffic to a DHCP-enabled interface.

  Workaround: There is no workaround.

- CSCsy73123

  Symptoms: Connected route on port-channel sub-interface is not removed when port-channel is down.

  Conditions: Happens when using /22 subnet. Does not happen when using /24 subnet.

  Workaround: There is no workaround.

- CSCsy73981

  Symptoms: Cisco AS5400 shows memory leak for DSMP, VTSP, and MGCP processes. Occurs about once a month.

  Conditions: After some time, the memory leak symptoms are seen on the gateway, although normal operations are not affected. Eventually all memory is consumed, and the gateway hangs. Only a manual reboot can bring it back to service.

  Workaround: There is no workaround.

- CSCsy74329

  Symptoms: The following message appears on the console:

  ```
  [crypto_bitvect_alloc]: bitvect full (size = 8192) -Traceback= 0x4244AB0 0x426875C
  0x426AE60 0x426B330 0x426FAF4 0x4292B7C 0x4293278 0x75429C
  ```

  Conditions: The symptom is observed when the GetVPN rekey is used with a number of Deny ACL entries and with VSA.

  Workaround: There is no workaround.

- CSCsy77191

  Symptoms: Native GigE interfaces of a Cisco 7200 NPE-G2 router will not acknowledge reception of pause frames and will not stop its transmission in case of media-type RJ45.

  Conditions: The symptom is observed with media-type RJ45 and with SFP with “no neg auto” configured.

  Workaround: There is no workaround.

  Further Problem Description: There are no issues with SFP with a “neg auto” configuration.

- CSCsy79301

  Symptoms: A router crashes when a multicast group address joins and leaves the MLD group from the client within the configured delay time.

  Conditions: The symptom is observed when applying MLD leave for the group for which accounting has not yet started.

  Workaround: There is no workaround.

- CSCsy79955

  Symptoms: Reverse SSH using PVDM2 modems fails. If the **ssh -l <username>:<line #> <ip>** command is entered, modem activation is triggered. The input of “atdt<number>” is making it to the modem, meaning whatever the <number> field is typed, it is reported in the debugs. However, the modem does not send anything back to router about it and no connection is made. At modem prompt, “at”, “at&f”, “ate1” (and perhaps others) do not appear to be taken.

  Conditions: Seen on routers running Cisco IOS Release 12.4(22)T and 12.4(23). Appears to be issue with all releases. Issue is seen when using both **ssh -l <username>:<line #> <ip>** and by using SSH from a client to a particular line.

  Workaround: There is no workaround.

- CSCsy81339

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

  Conditions: The reload happens when a QoS configuration change is made while a packet is in the middle of being processed on the interface where QoS is applied.

  Workaround:

  1. Shutdown the interface before making any QoS configuration changes.
  2. Remove the service policy from the interface while making the configuration change.

- CSCsy84286

  Symptoms: Router crashes while removing “ip dhcp class”.

  Conditions: The symptom occurs with relay agent information and relay-information hex configured.

  Workaround: There is no workaround.

- CSCsy88640

  Symptoms: A core dump may fail to write, with the following errors seen on the console:

```
current memory block, bp = 0x4B5400A0,
memorypool type is Exception
data check, ptr = 0x4B5400D0
bp->next(0x00000000) not in any mempool
bp_prev(0x00000000) not in any mempool
writing compressed ftp://10.0.0.1/testuncached_iomem_region.Z
[Failed]
writing compressed ftp://10.0.0.1/testiomem.Z
[Failed]
writing compressed ftp://10.0.0.1/test.Z
[Failed]
%No memory available
```

  Conditions: This is only seen for memory corruption crashes when “exception region-size” is configured to a value that is not divisible by 4.

  Workaround: The recommended setting for exception region-size is 262144 in newer images. In older images, where the maximum configurable value is 65536, use the maximum.

- CSCsy90542

  Symptoms: Multicast traffic is dropped at decrypting side.

  Conditions: This symptom occurs when traffic ACL on the KS is of the type:

  permit ip host *address* any permit ip any host *address*

  Workaround: There is no workaround.

- CSCsy91748

  Symptoms: An NM-CEM-4SER module crashes.

  Conditions: The symptom is observed with an NM-CEM-4SER module when its payload size is changed on a CEM port which is part of a multiplexed group that is created using the **attach <port>** command.

  Workaround: Reload the router after using the **write config** command.

- CSCsy93054

  Symptoms: WebVPN portal is not displayed. The router closes the SSL negotiation as soon as it sends an SSL “Server Hello” message by sending a TCP FIN.

  Conditions: The symptom is observed when a trustpoint uses a certificate chain of larger than 4096 bytes.

  Workaround:

  1. Use a smaller certificate chain.
  2. Use self-signed certificates.

- CSCsy97820

  Symptoms: False positives are seen in matching object groups with variable masks.

  Conditions: The symptom is observed when non-matching traffic is sent.

  Workaround: Do not use variable masks and contiguous masks, such as 255.0.255.255. Use only contiguous masks.

- CSCsz13123

  Symptoms: Frame-relay DLCI is not released from interface in a certain configuration sequence.

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS 12.4T images.

Workaround: There is no workaround.

- CSCsz14236

  Symptoms: LLC stops forwarding I frames, but continues to respond to poll frames.

  Conditions: The symptom is detected when the output from **show llc** shows that frames are queued up for transmission in the Tx Queue. If DLSw is transporting the LLC frames, the associated DLSw circuit will show that the link is in a max congestion state.

  Workaround: There is no workaround.

- CSCsz16635

  Symptoms: One-way audio may be experienced on a call which traverses a transcoder hosted on an ISR platform (e.g.: Cisco 2800, 3800 etc) after a hold, resume, or transfer.

  Conditions: When the call is held or resumed, there is a significant change in the RTP Sequence Numbers but the SSRC does not change. This behavior may cause the receiving device to assume that the RTP packets are out of sequence (i.e.: late, early, or lost) and therefore the receiving device may drop them.

  Workaround:

  1. A hold/resume from the phone receiving the out-of-sequence RTP audio packets will restore normal reception of audio.
  2. If possible, use a Communications Media Module (CMM) module for transcoding while ensuring that the Cisco IOS Release used on the CMM module has the fix for CSCsi27767.
  3. If possible, eliminate the need for a transcoder in the audio path for affected call flows.
  4. This problem does not affect Cisco IOS Software Media Termination Points (MTPs) nor SW MTPs hosted on a Cisco Unified Communications Manager (CUCM) server. So, if like-to-like capabilities (i.e.: codec and packetization) are being used, then using a SW MTP via IOS or CUCM may be an option.

  Further Problem Description: This issue looks very similar to CSCsi27767 which was opened and resolved against the Catalyst 6000's CMM. The fix for CSCsi27767 is, however, only intended for the CMM platform.

  IOS DSPFarm services and voice gateways will now avoid generating discontiguous RTP sequence numbers with the same SSRC, by using a new SSRC and setting the marker bit of the first RTP packet for the new SSRC whenever its DSP restarts the RTP sequence number due to call features such as call transfer, hold, resume, etc.

- CSCsz16941

  Symptoms: A TR-069 Agent becomes disabled on the router and the device is unreachable from the ACS server.

  Conditions: The symptom is observed when a TR-069 Agent is enabled and running on a router and the default WAN interface is configured and has a DHCP-assigned IP address. When the configurations are saved and the router is reloaded the issue is seen.

  Workaround: If possible, do not save the configurations on the router when the WAN interface gets a DHCP-assigned IP address.

  Alternate workaround: Use the **write erase** command and remove all the configurations just before every router reload.

- CSCsz20496

  Symptoms: A Cisco VG224 voice gateway displays the wrong secondary dialtone to the customer if "cptone CN" is configured under the voice-port.

Conditions: The symptom is observed with Cisco IOS Releases 12.4(24)T, 12.4(20)T1, and 12.4(9)T7.

Workaround: Upgrade to the latest IOS version (see bug CSCsk28301) and change the dial_tone2 to make it same as the dialtone by using the command **test voice tone cn 2nd_dialtone**:

```
event manager applet setCNsecondDialtone
  event syslog occurs 1 pattern ".*%SYS-5-RESTART: System restarted --.*"
  action 1.0 syslog msg "Setting DIAL_TONE2 for cptone CN"
  action 2.0 cli command "enable"
  action 3.0 cli command "test voice tone CN 2nd_dialtone 1 450 0 -100 -100 -100 0 0 0
0xFFFF 0 0 0 0 0 0 0"
  action 4.0 syslog msg "DIAL_TONE2 for cptone CN has been set"
```

Copy the script to the running-configuration and then save it to NVRAM. If the router reloads, the setting “test voice tone CN 2nd_dialtone 1 450 0 -100 -100 -100 0 0 0 0xFFFF 0 0 0 0 0 0 0" will automatically be re-asserted. If you want the command set immediately without a reload then cut and paste the command directly at the EXEC prompt.

- CSCsz23951

  Symptoms: NSAP address family cannot be configured.

  Conditions: The symptom is observed with the initial configuration.

  Workaround: There is no workaround.

- CSCsz23976

  Symptoms: A Cisco 7200 series router that is running Cisco IOS Release 12.4(15)T7 may experience an unexpected reset while forwarding traffic with a Cisco 7200 VSA.

  Conditions: The symptom is observed on a Cisco 7200 series router running with a Cisco 7200 VSA installed on Cisco IOS 12.4(15)T code.

  Workaround: There is no workaround.

- CSCsz29320

  Symptoms: A Cisco 3845 running Cisco IOS Release 12.4.(20)T2 reloaded due to software-forced crash while experiencing the following error:

  ```
  %SYS-6-STACKLOW: Stack for process MGCP Application running low, 0/12000
  %Software-forced reload
  ```

  Conditions: The crash suggests that the issue is just one of inefficient stack usage.

  Workaround: There is no workaround.

- CSCsz29815

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

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

  Workaround: Reload the router.

- CSCsz35632

  Symptoms: Router crashes @ vpi_att under low memory condition.

  Conditions: Router crashes while running the c7200-adventerprisek9-mz.124-20.T3 image.

  Workaround: There is no workaround.

- CSCsz38104

  The H.323 implementation in Cisco IOS Software contains a vulnerability that can be exploited remotely to cause a device that is running Cisco IOS Software to reload. Cisco has released free software updates that address this vulnerability. There are no workarounds to mitigate the vulnerability apart from disabling H.323 if the device that is running Cisco IOS Software does not need to run H.323 for VoIP services. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-h323.shtml.

- CSCsz45419

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

  Conditions: This happens on a Cisco router running an internal build of Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsz45567

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is posted at:

  http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

- CSCsz45855

  Symptoms: Cisco Unified Border Element (CUBE) ignores reINVITEs from Cisco Customer Voice Portal (CVP).

  Conditions: While call transfer is in progress and CUBE is waiting for NOTIFY (with 200 or any final response code) after receiving NOTIFY (with 100), it receives INVITE.

  Workaround: There is no workaround.

- CSCsz48392

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

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

  Workaround: There is no workaround.

- CSCsz48914

  Symptoms: Next Hop Resolution Protocol (NHRP) registration and tunnels are not up between first- and second-level hubs.

  Conditions: Occurs in hierarchical topology.

  Workaround: There is no workaround.

- CSCsz49741

  Devices running Cisco IOS Software and configured for Cisco Unified Communications Manager Express (CME) or Cisco Unified Survivable Remote Site Telephony (SRST) operation are affected by two denial of service vulnerabilities that may result in a device reload if successfully exploited. The vulnerabilities are triggered when the Cisco IOS device processes specific, malformed Skinny Call Control Protocol (SCCP) messages.

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCsz50275

  Symptoms: The firewall is configured to reset if an invalid command goes through the unit under test. But the reset action does not happen, and this functionality issue observed all inspected application traffic, such as IM, SIP, and P2P.

  Conditions: This problem occurs both when Cisco Common Classification Policy Language (C3PL) is used, and when it is not used.

  Workaround: There is no workaround.

- CSCsz52815

  Symptoms: If number of hours for statistics is increased to 10 or more after the probe is initially run and then restarted, system crashes with memory corruption

  Conditions: Occurs when the probe is started with the hours of statistics less than 10 and then re-started with the hours of statistics greater than 9.

  Workaround: There is no workaround.

- CSCsz53177

  Symptoms: When running Network Load-balancing (IGMP-mode) in VLANs with PIM enabled and static ARP entries for unicast IP to layer-2 multicast address, packet duplication will occur.

  Conditions: This symptom occurs when sending unicast (non-multicast) IP packets with multicast layer-2 destinations.

  Workaround: Use non-IGMP NLB modes (unicast or multicast with static MACs) or use IGMP snooping querier instead of PIM on NLB SVIs.

- CSCsz56169

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

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

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

- CSCsz58785

  Symptoms: When using the Cisco Service Selection Gateway (SSG) feature in Cisco IOS Release 12.4(22)T with TCP-Redirect and SSG Port Bundle Host Key (PBHK)/port-map, redirected packets may be dropped and not be forwarded to the Cisco Subscriber Edge Services Manager (SESM).

  Conditions: Occurs on a router running Cisco IOS Release 12.4(22)T and configured for SSG and with “ssg port-map” and “ssg tcp-redirect” configured.

  Workaround: There is no workaround known other than using an older IOS release or disabling port-bundle host key (PBHK).

- CSCsz58813

  Symptoms: Cisco UC500 console displays the following log(s) constantly:

%PQII_PRO_FE-4-QUEUE_FULL: Ethernet Switch Module transmit queue is full.

Phones and hosts connected to the UC can not retrieve IP addresses via DHCP.

Conditions: This problem occurs shortly after a reload of the Cisco UC500 (on the CME side). This problem is observed after upgrading from Cisco IOS Release 12.4(20)T2 to Cisco IOS Release 12.4(20)T3.

Workaround: There is no workaround.

- CSCsz60659

  Symptoms: The cooperative GDOI keyserver starts printing %GDOI-5-COOP_KS_REACH and/or %GDOI-5-COOP_KS_UNREACH syslog messages.

  Conditions: The symptom is observed if two or more ISAKMP connection attempts fail, which might be normal in production networks.

  Workaround: There is no workaround.

  Further Problem Description: In fixed versions, the logic of the reachability test was changed to avoid this problem.

- CSCsz63721

  Symptoms: CPU utilization goes to 90% or above when PfR is configured with a large number of policy using fastmode and forced target.

  Conditions: The problem is limited to a large number of forced target (greater than 500) and fastmode with probe frequency of 2-5 seconds. CPU usage progressively gets worse with the increase in number.

  Workaround: Use longest-match targets instead of forced targets. Forced targets are configured under oer-map, and longest-match targets are configured under OER master. Forced targets are required only if the target does not belong to the destination subnet of the traffic-class being optimized.

- CSCsz68373

  Symptoms: After configuring NAT, traffic fails to hit the policy-map of the frame-relay serial interface.

  Conditions: This issue is seen with NM-1T3/E3 of a Cisco 3845 router only when NAT is configured.

  Workaround: Remove and re-apply the frame-relay map-class under serial interface after NAT is configured.

- CSCsz69486

  Symptoms: A multicast video stream forwarded between GE0/0 subinterfaces is policed by the Control Plane Policing (CoPP) class-default. As soon as CoPP is removed, the video recovers its original quality.

  With CEF: qffsydbd6ar01#deb control-pl qffsydbd6ar01#sh log | i reason Control Plane: marking pak exception [cef reason 12] Control Plane: marking pak exception [cef reason 39]

  Without CEF: qffsydbd6ar01(config)#no ip cef qffsydbd6ar01#deb control-pl qffsydbd6ar01#sh log Control Plane:marking in pak exception [non cef linktype IP]

  Conditions: This occurs after upgrading to Cisco IOS Release 12.4(20)T2.

  Workaround: There is no workaround.

- CSCsz70486

  Symptoms: On a Cisco 7200 series router with a VPN Services Adapter (VSA) installed, the outbound interface Access Control List (ACL) is not checked if a crypto map is applied to the interface and Cisco Express Forwarding (CEF) is enabled globally.

  Conditions:

  1. Egress ACL configured on the interface.
  2. A crypto map is applied to the same interface.
  3. VSA is installed in the chassis.
  4. CEF is enabled.

  Workaround: Remove the VSA or the crypto map, or disable CEF.

- CSCsz71392

  Symptoms: WCCP stops functioning when GDOI SA is accelerated by VSA.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(24)T with VSA (FPD 0.23). It is seen when **ip wccp** *61* **redirect out** and **ip wccp** *62* **redirect in** are applied to the inside interface, and traffic gets WCCP GRE redirected to WAE. When GDOI crypto-map (currently in inbound-only state) is applied to the outside interface, traffic is returned from WAE via WCCP and GRE gets dropped within UUT.

  Workaround: Disabling VSA with **no crypto engine slot 0** restores connectivity to normal.

- CSCsz75186

  Cisco IOS Software is affected by a denial of service vulnerability that may allow a remote unauthenticated attacker to cause an affected device to reload or hang. The vulnerability may be triggered by a TCP segment containing crafted TCP options that is received during the TCP session establishment phase. In addition to specific, crafted TCP options, the device must have a special configuration to be affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability.

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

- CSCsz79001

  Symptoms: A Cisco 87x router may hang or crash after displaying “Now reloading” during ROMmon upgrade when using the **upgrade rom-monitor file flash:** command.

  Conditions: This occurs when a router running ROMmon release 12.3(8r)YI4 or an older ROMmon from alternate space is upgraded to YI5 or a newer ROMmon version

  Workaround: Power cycle the router to recover from this hang state. The router will then boot with the upgraded ROMmon.

- CSCsz79901

  Symptoms: Firmware file download using the TR-069 Agent on a router fails.

  Conditions: The symptom is observed when doing a firmware upgrade using the TR-069 Agent on a router and when the URL is given as “http://{ip address}/dir/filename.bin?{name}={value}”. This issue is noticed only with the TR-069/CWMP Agent.

  Workaround: Firmware download works if the URL is given as “http://{ip address}/dir/filename.bin”.

- CSCsz81308

  Symptoms: Using “send break” causes router to display ‘TLB Miss exception’ error and hang indefinitely.

Conditions: Occurs on a Cisco 800 router running Cisco IOS Release 12.4(24.6)T9.

Workaround: There is no workaround.

- CSCsz85919

  Symptoms: A router reloads with a SegV exception.

  Conditions: The symptom is observed with a router that is running Cisco IOS Release 12.4(20)T2 with both NAT and output ACLs configured. It occurs when the packet size changes due to NAT (this can happen with SIP/H.323 etc.).

  Workaround: There is no workaround.

- CSCsz86837

  Symptoms: After few days of normal operations, Cisco L2TP network server (LNS) starts rejecting significant percentage of L2TP sessions. While problem is present **debug vpdn l2x-event** shows:

  ```
  "312238: May 13 14:32:43.042: VPDN Tnl/Sn 0 0 CLIENT: fail to set server 000BA226 ->
  session 000BA226
  312239: May 13 14:32:43.042: VPDN Unknown vpdn syslog error due to AAA disconnect code
  0"
  ```

  Conditions: Occurs after a few days of LNS uptime.

  Workaround: There is no workaround.

- CSCsz92924

  Symptoms: CPU HOG in Crypto ACL is seen on the GM. The GM may crash some milliseconds later after printing the hog.

  Conditions: This symptom is observed on a large ACL on the KS (greater than 70 lines) with or without large ACL locally on the GM.

  Workaround: Limit the ACL length drastically.

- CSCsz93207

  Symptoms: In an EZVPN scenario, the traffic to the internet is not getting NATed.

  Conditions: The symptom is observed in an EZVPN scenario with “identical addressing” and “split tunnel” configured.

  Workaround: Use Cisco IOS Release 12.4(15)T3.

- CSCsz96323

  Symptoms: A Cisco 7301 router crashes with “protocol pptp” configured.

  Conditions: The symptom is observed with a Cisco 7301 router when “protocol pptp” is configured.

  Workaround: There is no workaround.

- CSCsz97833

  Symptoms: HTTP-based certificate revocation list (CRL) checking fails.

  Conditions: Occurs due to an extra character appended to the URL.

  Workaround: Disable CRL checking.

- CSCsz99228

  Symptoms: When the **clear crypto gdoi** command is issued on the GM in a setup where one GM and two KSs are used, a crash is seen on the GM. This does not happen before the **clear crypto gdoi** is used. Also, this crash was not seen in a setup involving just one GM and one KS.

  Conditions: This crash is only seen on Cisco IOS Release 12.4(20)T.

  Workaround: There is no workaround.

- CSCta00794

  Symptoms: %SYS-3-CPUHOG is seen when multicast fanout performance test is executed with a large number of IGMP or PIM joins and forwarding out through a large number of OIF (1000 sub-interfaces).

  Conditions: Observed on a Cisco 7200 router running Cisco IOS Release 12.4(24.06)T9.

  Workaround: There is no workaround.

- CSCta02089

  Symptoms: There is a crash on a Cisco AS5400 due to CPU signal 10.

  Conditions: The symptom is observed on a Cisco router due to expiration of freed receive_digit timer in SIP

  Workaround: There is no workaround.

- CSCta02460

  Symptoms: On a router that has a PRI trunk towards the PSTN, you may hear dead air when calling any ISDN device that returns cause code 0x8484 in a PROGRESS message that also contains a progress_ind with value 8.

  Conditions: The symptom is seen when using the primary-4ess (PRI 4ESS) and primary-5ess (PRI 5ESS) switch type.

  Workaround: There is no workaround.

  Further Problem Description: The problem was discovered when a user attempted to call a cell phone on a wireless network that was switched off. The user did not have voicemail, and the wireless network played a message in the band to alert that the phone was off. It is this message that should be heard - but it is not, due to this bug.

  The issue is due to an invalid cause value sent from the provider for an outgoing to call to a mobile phone which is switched off. The cause value of 4 is not supported by PRI 4ESS switches. Hence ISDN will send a STATUS message reporting invalid information element contents and the provider disconnects the call.

- CSCta04123

  Symptoms: A router may crash with a “STACKLOW” message or memory corruption.

  Conditions: The symptom is observed when the router is configured for IP inspect (only a basic IP inspect configuration is necessary).

  Workaround: Disable IP inspect.

- CSCta04391

  Symptoms: Router with dynamic NAT for unicast and multicast traffic crashes after deleting **ip nat inside source list**.

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

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

- CSCta12296

  Symptoms: Group member router crashed.

  Conditions: Occurs when unicast re-keys are received frequently (TEK 300).

  Workaround: There is no workaround.

- CSCta25832

  Symptoms: Intermittent call failures occur through a Cisco AS5350XM or AS5400XM gateway.

  Conditions: The gateway is configured as an ISDN gateway. The **show voice call summary** command will show b-channels stuck as shown below:

  #show voice call summary

```
PORT            CODEC      VAD VTSP       STATE      VPM     STATE
3/6:D.13        g711ulaw    n  S_CONNECT S_TSP_WAIT_RELEASE
```

  This is usually seen after the gateway has processed a very high number of calls (~200,000 calls or more).

  Workaround: There is no workaround.

- CSCta35393

  Symptoms: CPE WAN Management Protocol (CWMP) agent on a Cisco Unified CallManager Express (CME) causes CPU to spike to 96%.

  Conditions: The symptom is observed when configuring the CWMP agent and placing a phone call.

  Workaround: Disable the CWMP agent.

- CSCta39579

  Symptoms: VPN routing/forwarding (VRF) Network Address Translation (NAT) is not translating UDP traffic at all. The inside local IP is still used after NAT. If the inside local IPs are not routable on the NAT outside side of the network this breaks all applications relying on UDP. ICMP and TCP traffic are not impacted

  Conditions: Occurs when NAT is inside a VRF. nat is in vrf

  Workaround: Make sure the inside local is known on the NAT outside side of the network.

- CSCta39763

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

  MJH-VG01# **show memory all totals**

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

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

  Workaround: There is no workaround.

- CSCta43033

  Symptoms: Cisco Unified Border Element (CUBE) gives OLC reject during transfer despite correct codec negotiation. The cause code is 57.

  Conditions: Occurs under reasonable load and with many call transfers (such as CVP or IPCC environment).

  Workaround: There is no workaround.

- CSCta45116

  Symptoms: EAP-FAST authentication fails between router and client (PC or laptop running ADU).

  Conditions: The symptom is observed when the wireless client is running “ADUv2.x” and the router is running with Cisco IOS Release 12.4(15)T8.

  Workaround: Upgrade the wireless client ADU to version 3.x or 4.x.

- CSCta45845

  Symptoms: All show commands under crypto are showing blank outputs. For example **show crypto pki certificates** shows a blank output, even though there may be some crypto certificates on the device.

  Conditions: This happens only when using web interface to an IOS device. The commands are:

```
7200-12-3#sh crypto pki ? certificates
Show certificates counters
Show PKI Counters crls
Show Certificate Revocation Lists server S
how Certificate Server session
Show PKI Session Data timers
Show PKI Timers token
Show PKI Token(s) trustpoints Show trustpoints
```

  Workaround: There is no workaround.

  Further Problem Description: CCA uses HTTP(s) service to get the output. Even when the certificate is shown using telnet/SSH, CCA GUI shows as unconfigured.

- CSCta46486

  Symptoms: CPU hogging in IKE and traceback seen on headend router terminating large amount of DVTIs.

  Conditions: The symptom is observed with any kind of outage on the remote site or clearing large amount of tunnels with the headend router actively participating in the routing and re-distributing the routes learned via the tunnel to the central site.

  Workaround: There is no workaround.

- CSCta49146

  Symptoms: Ping fails when mandatory certificate revocation list checking is enabled.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(20)T4.

  Workaround: There is no workaround.

- CSCta65793

  Symptoms: Router crashes while configuring “no auto-summary” in EIGRP at startup.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS 12.4M and 12.4T images.

  Workaround: As the router processes the auto-summary command prior to any interfaces participating in EIGRP becoming fully established, the workaround is to defer configuring the auto-summary command until after interfaces have been fully enabled and are participating in EIGRP.

- CSCta68917

  Symptoms: Cisco IOS allows duplicate installation of the same SSL VPN Client (SVC) packages with different sequence numbers.

  Conditions: Because of this defect, uninstallation of the SVC package causes an error when the same package has been installed more than once.

  Workaround: Install a SVC package only once on the router with the required sequence number.

- CSCta69118

  Symptoms: The ping from CE1 to CE2 fails when VLAN xconnect is provisioned, even though the session is up.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(20)T4.

Workaround: There is no workaround.

- CSCta75271

  Symptoms: When we change a policy-map from a pure precedence policy (only match precedence classes) to a pure DSCP policy (only match DSCP classes), it causes a crash.

  Conditions: When we remove the last precedence/DSCP class from a pure policy and replace it with DSCP/QoS_group, it causes a crash. Occurs in Cisco IOS Release 12.4(20)T and 12.4(24)T throttles.

  Workaround: Remove the service-policy from the interface, then make the change to the policy-map and reapply the service-policy on the interface again.

- CSCta79634

  Symptoms: System crash in L2TP. Following this, most of the L2TP setups fail.

  Conditions: The symptom occurs at an L2TP control-plane event.

  Workaround: Clear VPDN again or reload the router.

- CSCta91556

  Symptoms: Packets are getting SSS switched on the LAC towards LNS.

  Conditions: The symptom is observed when bringing up any PPPoE or PPPoA session.

  Workaround: There is no workaround.

- CSCtb14400

  Symptoms: Packets received from the virtual-access CE-facing interface are not CEF-switched into the MPLS cloud.

  Conditions: The symptom is observed on a MPLS/VPN PE router.

  Workaround: There is no workaround.

- CSCtb45948

  Symptoms: Entering **ntp ?** at the router command prompt does not enable **server** and **peer** options to be configured.

  Conditions: The **ntp server** and **ntp peer** commands cannot be configured.

  Workaround: There is no workaround.

- CSCtb48852

  Symptoms: Multilink Frame Relay (MFR) bundle in HW mode.

  Conditions: Occurs when different PA members are added to MFR on a Cisco 7200 router.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(20)T3

Cisco IOS Release 12.4(20)T3 is a rebuild release for Cisco IOS Release 12.4(20)T. The caveats in this section are resolved in Cisco IOS Release 12.4(20)T3 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCsg84765

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

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

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

  Workaround: There is no workaround.

- CSCsi43340

  Symptoms: DSMP is not programming the DSP for supervisory tone while alerting tone is there, which leads to FXO disconnect supervision issue.

  Conditions: Occurs on routers running Cisco IOS Release 12.3(14)T and later releases.

  Workaround: Downgrade to Cisco IOS Release 12.3(11)T.

- CSCsj93465

  Symptoms: A PRE-3 may crash at the “pppatm_pas_fs” function.

  Conditions: This symptom is observed on a Cisco 10000 series that runs the c10k3-p11-mz image of Cisco IOS Release 12.2(31)SB1 and that is configured for PPP. The symptom occurs after a write operation. The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCsk43926

  Symptoms: High CPU usage may occur interrupt context on an RP, and spurious memory accesses may be generated when a route-map update is checked. You can verify this situation in the output of the **show align** command.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for BGP.

  Workaround: There is no workaround.

- CSCsk45399

  Symptoms: A device might crash when the QoS configuration is changed.

  Conditions: This symptom is observed on a device that has a QoS configuration.

  Workaround: There is no workaround.

- CSCsl46159

  Symptoms: When the cost-minimization feature is used in OER, prefixes are moved to minimize the cost, but it never reaches a stable point. In other words, prefixes are moved back and forth periodically.

  Conditions: This symptom is observed only if OER cost-minimization is configured.

  Workaround: There is no workaround.

- CSCsm92992

  Symptoms: Brand new NVRAM chips will not have the magic numbers written for the primary, backup, and secondary backup NVRAM. This will cause error messages when trying to read/write to the NVRAM (see below).

```
Router#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvramwr
Building configuration...
[OK]
Bad configuration memory structure -- try rewriting
Bad configuration memory structure -- try rewriting
Router#
Router#
Router#wr
Bad configuration memory structure -- try rewriting
Bad configuration memory structure -- try rewriting
Building configuration...
[OK]
Bad configuration memory structure -- try rewriting
Bad configuration memory structure -- try rewriting
Router#
```

  Workaround: Load an image older than Cisco IOS Release 12.4(20)T, which will write the magic numbers. Then load an image from Cisco IOS Release 12.4(20)T or a later release.

- CSCso40618

  Symptoms: A Cisco 871 router may crash with error %SYS-2-NOTQ with Process="DNS Resolver" after loading an image.

  Conditions: Firewall application inspection for IM protocols is configured. Protocol-info parameter-map is configured to resolve the IM server host names and is associated to IM protocols in firewall class-map.

  Trigger: Issue is caused when router uses "parameter-map protocol-info" which has a list of IM server host names, to resolve list of IM servers.

  Workaround: Do not associate the protocol-type parameter-map to IM protocol in firewall class-map.

- CSCsq24002

  Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml.

- CSCsr23454

  Symptoms: A device reloads with a bus error and may display the following message:

```
CMD: ' aggregate-address 224.0.0.0 224.0.0.0 attribute-map GCI-aggregations
suppress-map Suppress-ESNAK' 16:19:05 GMT Wed Jun 18 2008

 16:19:06 GMT Wed Jun 18 2008: Address Error (load or instruction fetch)
exception, CPU signal 10, PC = 0x60CDD444
```

  Conditions: The symptoms are observed on a device configured with Border Gateway Protocol (BGP).

  Workaround: There is no workaround.

- CSCsr27727

  Symptoms: A Cisco Catalyst 6000 reports the following message and unexpectedly reloads:

  ```
  %SYS-2-ASSERTION_FAILED: Assertion failed: "wccp_acl_item_valid(item,NULL)"
  ```

  Conditions: This symptom is observed on a WS-C6509 that is running Cisco IOS Release 12.2(33)SXH2a.

  A WCCP service is configured with a redirect-list referring to a simple ACL.

  Workaround: Use an extended ACL as the WCCP redirect-list.

- CSCsr41631

  Symptoms: AnyConnect client is connecting to a Cisco ISR router that is running Cisco IOS Release 12.4(20)T with hardware encryption and CEF enabled. Client is unable to reach the inside interface IP address but can communicate with devices behind the router.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(20)T with hardware encryption and CEF enabled

  Workaround: Disable CEF globally and/or disable hardware encryption.

- CSCsr44382

  Symptoms: Add-on modules (7914/7915/7916) are not showing correct shared line status after registering.

  Conditions: This symptom occurs when the add-on module has a shared line configured on it, and the add-on module has just recently registered. The share line status on the add-on module is not updated after add-on registers.

  Workaround: There is no workaround.

- CSCsr50834

  Symptoms: A CPU hog may be seen after changing the “logging buffered” setting to up to 50MB or more. This issue can cause an OSPF flap.

  Conditions: The symptoms are observed with Cisco IOS Release 12.2(33)SXH2 on a Cisco WS-C6506.

  Workaround: Instead of manipulating such a large logging buffer at runtime when the device/network is busy, consider configuring the “logging buffered” setting once and save it as part of the startup configuration. This way, the huge logging buffer will be allocated during the device initialization without runtime impact.

- CSCsr51801

  Symptoms: Some of the route-maps configured for BGP sessions (eBGP) are not permitting the prefixes upon a router reload.

  Conditions: The symptom is observed when a large number of route-maps for a BGP session are configured and the router is reloaded.

  Workaround: Issue the command **clear ip bgp * soft**.

- CSCsr65069

  Symptoms: A router reports “%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header” and reloads.

  Conditions: This symptom is observed with Cisco routers that are running Cisco IOS Release 12.4T under an increased traffic load.

  Workaround: There are no known workarounds.

Further Problem Description: This issue is related to a classification engine in Cisco IOS software. This engine is used by all features that require classification (for example, QoS, NetFlow).

- CSCsr97753

  Symptoms: Pinging an interface fails.

  Conditions: Occurs when unconfiguring xconnect on the interface.

  Workaround: Perform a **shut/no shut** on the interface.

- CSCsu02975

  Symptoms: A router crashes due to memory corruption.

  Conditions: A WAN router crashes when feature combination including Frame Relay, EIGRP, GRE, QoS, and multicast are configured on WAN aggregation and branches.

  The issue is seen only on PA-MC-2T3/E3-EC and only when frame-relay fragment and service-policy is part of map-class frame-relay configurations.

  Workaround: Have either frame-relay fragment or service-policy as part of map-class frame-relay configurations.

- CSCsu38520

  Symptoms: In Cisco IOS Release 12.4(20)T and 12.4(15)T7, IKE Phase 1 is not flushed by DPD (although IKE Phase 2 is correctly deleted). This can be verified by using the following commands:

  show crypto isakmp sa then **show crypto ipsec sa**
  Conditions: The symptom is observed when the IPSec end node is behind NAT and DPD is configured. It is seen when the last IKE Phase 2 SA is deleted.

  Workaround: Use Cisco IOS Releases up to 12.4(15)T6.

- CSCsu65401

  Symptoms: Commands run using the **tclsh** exec command fail with the error**:**

  ```
  Command authorization failed.
  ```
  Conditions: This occurs in Cisco IOS Release 12.4(20)T if the following is configured on the device:

  aaa authorization commands 15 default group tacacs+

  Workaround: The username being passed to the AAA server is an empty string. If there is a default profile on the AAA server that allows all commands to be run, then the **tclsh** exec commands will work. Otherwise there is no workaround.

- CSCsu71818

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

  Conditions: Occurred on a Cisco 7206VXR (NPE-G1) that is very busy running NAT. The router crashed with the following Cisco IOS Release 12.4(16a) and 12.4(15)T1.

  Workaround: There is no workaround.

- CSCsu95080

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

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

  Workaround: Configure MLD.

- CSCsv20948

  Symptoms: The primary router may crash continually.

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

Workaround: There is no workaround.

- CSCsv27607

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

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

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

- CSCsv28451

  Symptoms: A Cisco 7600 PE router fails to redistribute a VRF prefix into BGP after the prefix or path to it flaps. The PE router will indicate the prefix being redistributed into BGP but the prefix will not get installed into the BGP table until the prefix is cleared:

```
PE2#
PE2#sh ip route vrf foo 10.5.5.5

Routing Table: foo
Routing entry for 10.5.5.5/32
  Known via "ospf 1", distance 110, metric 20, type extern 2, forward metric 10
  Redistributing via bgp 666
  Advertised by bgp 666 metric 10 match internal external 1 & 2
  Last update from 10.45.45.2 on Ethernet1/0, 00:00:56 ago
  Routing Descriptor Blocks:
  * 10.45.45.2, from 10.5.5.5, 00:00:56 ago, via Ethernet1/0
      Route metric is 20, traffic share count is 1
PE2#
PE2#sh ip bgp vpnv4 vrf foo 10.5.5.5
% Network not in table
PE2#
```

  Conditions: The PE router redistributing the given prefix must have a sham-link configured for the given VRF and an alternate path to the prefix must exist once the primary (sham-link) is down.

  Workaround: Use the following command: **clear ip route vrf vrfname** *prefix*.

  Further Problem Description: This problem is seen only in Cisco IOS Release 12.2(33)SRB. Cisco IOS Releases 12.2(33)SRC/SRD, etc. are not affected.

- CSCsv29659

  Symptoms: RP configured inside a NAT not shown on test device outside the NAT.

  Conditions: Entering the **show ip pim rp mapping** command fails to display the RP.

  Workaround: There is no workaround.

- CSCsv31812

  Symptoms: Version: disk2:c7200-adventerprisek9-mz.124-22.T on KSs and GMs:

```
%GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for
group DGVPN-ALPHA from address 10.32.178.56 to 239.192.1.190 with seq # 23
```

```
%SYS-3-MGDTIMER: Uninitialized timer, set_exptime, timer =
20A64C70.
-Process= "Crypto IKMP", ipl= 0, pid= 201,
-Traceback= 0x6147CC48
0x62E75F4C 0x6392E05C 0x6392E300 0x63B25A70 0x63B25AF8 0x639308FC 0x63855544
0x6392F794 0x638100F4 0x638144E4
```

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

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

Workaround: There is no workaround.

- CSCsv49359

  Symptoms: In a scenario where a Cisco 7200 with NPE-400 is used to terminate AnyConnect clients on one side and MPLS VPN on another side, the return packets are never forwarded to the client and tracebacks are produced for every single packet.

  Conditions: Occurs with the following configuration:

  - Full SSL tunnel on one end
  - Packets coming as MPLS labeled packets
  - Cisco 7200 with NPE-400

  Workaround: There is no workaround.

- CSCsv62777

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

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

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

- CSCsv64889

  Symptoms: TCP traffic to a router interface is corrupted if the traffic is going through WebVPN with SVC or AnyConnect.

  Conditions: Occurs with AnyConnect or SVC connection and traffic destined to a router interface.

  Workaround: Use IPSec.

  Further Problem Description: The traffic does not fail immediately, but after around 7 seconds.

- CSCsv66215

  Symptoms: Problem with IPv6 when deactivating and then reactivating VPN routing/forwarding (VRF).

  One symptom is a message “Can’t activate address-family ipv6”.

  Another aspect is a reference to tableid 10000000 that is reserved and should not apply to VRF.

  Conditions: This symptom occurs when using VRFs. The problem only occurs if IPv6 routing is used and then fully removed. When IPv6 is removed from the system, the IPv6 RIB goes away. One way of reactivating the IPv6 RIB is to indirectly create some VRFs. In that case, it is possible that the tableid 10000000 be allocated to a VRF, and the problem occurs.

Workaround: The path that leads to the problem consists in allocating the IPv6 RIB indirectly via VRFs installation. The problem only occurs at reactivations. See the following workarounds:

- Reboot the router.
- Configure **ipv6 unicast router** or IPv6 on interfaces before entering VRF configuration.

- CSCsv66513

  Symptoms: When an external interface is shutdown (on a controlling border router) all the applications (controlled) on that interface do not go to DEFAULT state.

  Conditions: The symptom is observed when PfR is enabled with applications that are configured to be controlled. It is seen when more than one application that is controlled (on same border router) exits.

  Workaround: There is no workaround.

- CSCsv66827

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

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

  Workaround: There is no workaround.

- CSCsv69784

  Symptoms: A middle buffer leak is observed when using the combination of RIP and multipoint frame relay.

  Conditions: Currently the trigger is unknown.

  Workaround: There is no workaround.

- CSCsv77531

  Symptoms: A device that is running affected versions of Cisco IOS software may reload.

  Conditions: This symptom occurs when the device is performing either CBAC traffic inspection or Zone Based Firewall Inspection on TFTP.

  See the following example of vulnerable configuration for CBAC traffic inspection:

```
!
! TFTP inspection rule is configured.
!
ip inspect name example_name tftp
!
! Apply inspection rule to the interface
!
interface Ethernet1/1
ip inspect example_name in
!
```

  Further information on CBAC is available at:

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_content_ac_ps6350_TSD_Products_Configuration_Guide_Chapter.html

  See the following example of vulnerable configuration for Zone-Based Policy Firewall inspection:

```
!
! Create a CBAC Class Map
!
class-map type inspect match-all tftp-traffic
```

```
 match protocol tftp
 match access-group 100
!
! Create a CBAC Policy Map
!
policy-map type inspect tftp-inspection
 class type inspect tftp-traffic
  inspect
!
```

Further information on Zone-Based Policy Firewalls is available at the following link:

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a008060f6dd.html

Workaround: Disable ios-firewall inspection for TFTP.

- CSCsv77932

  Symptoms: Router crashes.

  Conditions: Occurs while configuring serial interface for insufficient MTU.

  Workaround: There is no workaround.

- CSCsv79584

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

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

  Workaround: There is no workaround.

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

- CSCsv81176

  Symptoms: Router crashes with syslog CHUNKBADMAGIC.

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

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

- CSCsv85530

  Symptoms: When accounting is enabled for virtual private dial-up network (VPDN), there might be messages with termination cause “nas-error” and displaying impossible values in Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets and Acct-Output-Packets.

  This causes accounting to be unreliable.

  Conditions: Occurs with Cisco IOS Release 12.4T and configured for PPTP/L2TP with accounting.

  Workaround: There is no workaround.

- CSCsv90106

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

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

Workaround: There is no workaround.

- CSCsv91602

  Symptoms: Cisco 7201 with Gi0/3 experienced communication failure.

  Conditions: This problem does not occur with Gi0/0 or Gi0/2.

  Workaround: Perform a **shut/no shut** on the Gi0/3. The problem will occur again.

- CSCsv96757

  Symptoms: After configuring random detect (WRED) on the ATM interface on a Cisco 888 Integrated Services router and traffic is sent through the VLAN input interface the to ATM interface, the router will display a continuous maclloc error. Additionally, the router crashes within 10-20 seconds after the traffic is stopped.

  Conditions: The problem is only observed on Cisco 888 Integrated Services router when WRED is enabled on the ATM interface.

  Workaround: Do not enable WRED on the ATM interface on the Cisco 888 Integrated Services router.

- CSCsv97772

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

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

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

- CSCsw14681

  Symptoms: The Sync Timer is not running after using the command **clear crypto gdoi**.

  Conditions: The symptom is observed with the following steps:

  1. Configure two cooperative KSs.
  2. Use the Cisco IOS 12.4(23.7)T image.
  3. Either reload or issue the **clear crypto gdoi** command in both routers.
  4. Let the election process complete.
  5. When the **sh crypto gdoi ks replay** command is issued, the following is shown:

```
%GDOI-5-COOP_KS_ELECTION: KS entering election mode in group GetvpnAdvanced1 (Previous
Primary = NONE)
%GDOI-5-COOP_KS_TRANS_TO_PRI: KS 10.10.1.1 in group GetvpnAdvanced1 transitioned to
Primary (Previous Primary = NONE)
KS1#sh crypto gdoi ks replay
Anti-replay Information For Group GetvpnAdvanced1:
  Timebased Replay:
    Replay Value             : 89.01 secs
    Remaining sync time      : Timer is not running <------------

Anti-replay Information For Group GetvpnAdvanced2:
  Timebased Replay:
    Replay Value             : 70.36 secs
    Remaining sync time      : Timer is not running <--------------------
```

```
Anti-replay Information For Group GetvpnAdvanced3:
  Timebased Replay:
         is not enabled
```

Workaround: There is no workaround.

- CSCsw21960

  Symptoms: A router crashes while executing some NAT commands.

  Conditions: The symptom is observed under the following conditions:

  - Try and configure “inside destination translation” with the command before configuring the pool or the access list “ip nat inside destination list ABC pool poo1”.
  - While you configure the above, keep traffic ON.
  - Make sure some active dynamic translations are present while you are configuring this.

  The router does not crash all the time. A combination of the above commands and removing and reconfiguring with traffic can cause the router to crash

  Workaround: There is no workaround.

  Further Problem Description: The crash is not consistently reproducible.

- CSCsw22791

  Symptoms: The router may crash if Group Domain of Interpretation (GDOI) configurations are removed concurrently with the execution of the **show crypto gdoi** command (that is, they are running on different TTY sessions).

  Conditions: The symptom is observed when the removal of the configurations and the execution of the show command are concurrent.

  Workaround: Avoid removing the configuration and executing the **show crypto gdoi** command concurrently.

- CSCsw24542

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

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

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

  Workaround: There is no workaround.

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

- CSCsw24611

  Symptoms: A router configured with BGP and VPN import may crash.

  Conditions: This is a hard to hit race condition. BGP imports a path from VRF-A to VRF-B. The following steps have to take place in exactly this order for the crash to occur:

  1. The next-hop for the path has to become unreachable.
  2. BGP has to re-evaluate the bestpath on the net in VRF-A and result in no-bestpath on the net (because there is no alternative path available).
  3. RIB installation has to process the importing BGP net under VRF-B.

Step 3 will result in the crash. If, before step 3, the next-hop re-evaluation manages to process the net in VRF-B then it will clear the bestpath and there will be no crash. If, before step 3, the import code gets a chance to process the net it will clean-up the imported path from VRF-B and then there will be no crash.

Workaround: There is no workaround.

- CSCsw24966

  Symptoms: SSL VPN client or AnyConnect client performance drops after a period of operation.

  Conditions: Occurs when Cisco Express Forwarding (CEF) is enabled.

  Workaround: Disable CEF if possible.

- CSCsw29463

  Symptoms: The router, which is configured as a hub in a Dynamic Multipoint VPN (DMVPN), may reload unexpectedly.

  Conditions: The symptom is observed periodically in a scaled configuration when the router is connected to a live network and traffic is passing.

  Workaround: There is no workaround.

- CSCsw29842

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

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

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

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

- CSCsw36397

  Symptoms: VoIP RTP connections may dangle at TGW when a call failure occurs, due to a performance test.

  Conditions: The symptom is observed during performance testing with many calls (more than 600) run for any duration above 5 minutes. The call failure occurs due to a network timeout issue from SIP server (acting as proxy server) causing hung VoIP connections at the TGW.

  Workaround: There is no workaround.

  Further Problem Description: The problem appears when the SIP server in the network delays responding to the messages sent from OGW and TGW due to network delays. The TGW is unable to clear the VoIP RTP sessions causing the hung RTP connections. If the calls run for more than an hour, the memory gets exhausted in the TGW causing it to crash.

- CSCsw42244

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

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

  Workaround: There is no workaround.

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

- CSCsw43211

  Symptoms: Following errors are seen:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_to_ptr (bad id) (id: 0xFFFFFFFF)
  -Traceback= 60476EBC 60477400 60491664 616C5834 616C7EEC 61AB72CC 61AC2E64 61AC2EBC
  60FE4274 60FDEFA4 60FD4180 60FD4874 60FD4BBC 60FD275C 60FD27A0 60FC8F74
  ```

  Conditions: This has been seen on a Cisco 7200 after upgrading to Cisco IOS Release 12.2(33)SRC2.

  Workaround: There is no workaround.

- CSCsw45320

  Symptoms: Router crashes after it has shown many tracebacks:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=xyz, count=0,
  -Traceback= ...
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=xyz, count=0,
  -Traceback= ...
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=xyz, count=0,
  -Traceback= ...
  ```

  Conditions: Router is terminating SSLVPN client sessions.

  Workaround: There is no workaround.

- CSCsw47543

  Symptoms: A router may loses all its free memory and crash.

  Conditions: The symptom is observed when the voice mail system sends a notification to the gateway regarding the availability of any voice messages. The memory leaks occurs in CDAPI_RawS.

  Workaround: Use the command **signalling forward none** under the global configuration “voice service voip”.

- CSCsw49297

  Symptoms: Packet drops and/or delays are observed when sending traffic over a multilink bundle interface.

  Conditions: This symptom may occur during periods of bursty traffic.

  Workaround: Increase the amount of data that a multilink will queue to a member link at any given time using the interface configuration command **ppp multilink queue depth qos** (default = 2). This command may be configured on the serial interfaces or, if the interface is a multilink group member, it may be configured on the multilink interface. For example:

  ```
  interface Multilink1
    ppp multilink queue depth qos 3
  ```

- CSCsw50802

  Symptoms: No extra I/O memory is allocated for some HWICs.

  Conditions: Occurs when HWIC is equipped with smart cookie.

  Workaround: Use static I/O memory configuration instead.

- CSCsw51214

  Symptoms: An Secure Real-Time Transfer protocol (SRTP) call may fail through a Cisco Multiservice IP-to-IP Gateway (IPIPGW).

  Conditions: The symptom is observed when a SRTP call is made between two Cisco Unified CallManager (CCM) with an IPIPGW in between.

  Workaround: There is no workaround.

- CSCsw52416

  Symptoms: Dynamic NAT entries are not timing out properly

  Conditions: Occurs even after timer expired.

  Workaround: There is no workaround.

- CSCsw52932

  Symptoms: Group members' rekey SAs that have the same IKE SA endpoints (source/destination addresses) are mistakenly deleted when one of the group members has to re-register.

  Conditions: This occurs when one of the group members has to re-register.

  Workaround: Have all the group members re-register at the same time (e.g. reapply the crypto map or use the **clear crypto gdoi** command).

- CSCsw62997

  Symptoms: Traceback is seen while configuring a policy in the virtual-template on LAC.

  Conditions: The symptom is observed when the class-map under the policy has the following filter:

  match vlan <vlan-id>

  Workaround: There is no workaround.

- CSCsw66082

  Symptoms: A router crash may be seen at ip_mcast_address_lookup when issuing the **show ip igmp ssm-mapping** *multicast group* on an SSM-mapping enabled router which makes use of DNS lookup for source list.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(23.10)T.

  Workaround: There is no workaround.

- CSCsw68022

  Symptoms: A router crashes after unconfiguring SCCP group using the following command: **no sccp ccm group #**.

  Conditions: The symptom is observed when SCCP group is configured on the router, and DSPfarm profiles (conference and transcoding) are configured and active on the router. If the commands **no sccp ccm group #** and **dspfarm profile <id> conference** followed by **shutdown** are entered at the same time, the router crashes.

  Workaround: Do not enter the commands **no sccp ccm group #** and **dspfarm profile <id> conference** followed by **shutdown** at the same time.

- CSCsw69069

  Symptoms: During the session, assigned IP address of the client changes, and after the session is finished only the last IP address is released. This causes IP pool exhaustion, which can be solved only by a reload.

  Conditions: Occurs on AnyConnect client on Cisco IOS Release 12.4(22)T.

Workaround: There is no workaround.

- CSCsw70204

  Symptoms: WISPr attributes could cause memory leak in ProxyLogon situation.

  Conditions: The symptom is observed when the subscriber logs on using WISPr attributes.

  Workaround: There is no workaround.

- CSCsw77293

  Symptoms: Upon unconfiguring “channel-group” in one controller, the ping fails in another controller.

  Conditions: The symptom is observed when a controller is configured and then unconfigured with “channel-group”.

  Workaround: Configure “channel-group” again.

- CSCsw78413

  Symptoms: The BFD configuration may be lost from the interface/sub-interface upon a router reload or physical module of OIR.

  Conditions: The symptom is seen when BFD is configured on an interface in certain multi-slot chassis.

  Workaround: Ethernet interfaces seem immune to this problem. Certain platforms, such as the Cisco 10000 series router, are also immune.

- CSCsw78879

  Symptoms: The secondary key server crashes when it sends a KEK rekey to the GMs soon after it takes over as the primary key server.

  Conditions: The symptom is seen when the secondary key server switches to primary just before it is time to send the KEK rekeys to the group members. This problem can be seen in any co-operative key server environment.

  Workaround: There is no workaround.

- CSCsw79696

  Symptoms: A call over the FXO loop-start cannot be established as the gateway’s DSP detects a reverse-battery signal.

  Conditions: The symptom is observed when the far-end is able to generate a reverse-battery signal when the called side is ringing. In addition, it is seen when “supervisory disconnect” is configured to either anytone or dualtone.

  Workaround: There is no workaround.

- CSCsw90055

  Symptoms: An FXO port with “supervisory disconnect tone” configured is unable to be released while receiving disconnect tone.

  Conditions: The symptom is observed when FXO is handling a fax call which will disable the FXO port “supervisory disconnect tone” capability and cause the FXO to be unable to detect the disconnect tone.

  Workaround: There is no workaround.

- CSCsw93682

  Symptoms: The KS database becomes unreliable.

Conditions: The symptom is observed when clearing the GM database from KS and re-registering GMs with different criteria.

Workaround: There is no workaround.

- CSCsw95531

  Symptoms: If hook flash occurs during a call that is not connected, interaction between gateway and CallManager will cause large number of zero duration call detail records to be written.

  Conditions: This symptom occurs on a Cisco VG224 that is running SCCP STCAPP and with Callmanager 4.2.

  Workaround: There is no workaround.

- CSCsw97665

  Symptoms: All www sites are allowed even though there is a matching local URL filter blocking policy configured, and the allow mode is set to off.

  Conditions: The symptom is observed when the local URL filter blocking policy is configured and the allow mode is set to off. Also, global CEF switching path is turned on.

  Workaround: There is no workaround.

- CSCsw98414

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

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

  Workaround: There is no workaround.

- CSCsw99846

  Symptoms: With mLDP over a P2P tunnel, traffic drops in multiple cases.

  Conditions: The traffic drops when there is a change in path set entries, which can happen when you perform a **shut** and **no shut** the TE tunnel or toggle MPLS traffic-tunnel or use the **clear mpls traffic-eng auto-tunne** command.

  Workaround: There is no workaround.

- CSCsx06457

  Symptoms: A router configured with BGP may generate IPRT-3-NDB_STATE_ERROR log messages. An additional symptom when **bgp suppress-inactive** is configured is that the router CPU usage may get close to 100%.

  Conditions: When both BGP and an IGP are advertising the same prefix, the error condition may occur. When in addition **bgp suppress-inactive** is configured high CPU usage by BGP may be seen.

  Workaround: Removing the **bgp suppress-inactive** configuration should eliminate the high CPU problem. Removing either the BGP or IGP conflicting routes from the system should clear both symptoms.

- CSCsx07114

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsx07423

  Symptoms: The router stays at 100% CPU usage after trying to establish an SSL session with an SSL server when this SSL server is not reachable.

  Conditions: The symptom is observed with any applications on the router that use an SSL client to establish a secure session with the SSL server. At the same time, the secure server is not available for whatever reason.

  Workaround: Make sure the SSL server is reachable by pinging it. Save the configuration as startup-config and reload the router.

- CSCsx09343

  Symptoms: PKI daemon is stuck in DNS resolution attempt for the hostname used in the CDP.

  Conditions: The symptom is observed when using name resolution for automatic actions taken by the router during non-interactive sessions (CRL download using name in CDP URI). This issue has been seen to occur only on a Cisco Catalyst 6500 running Cisco IOS SXH software.

  Workaround: There is no workaround.

- CSCsx15358

  Symptoms: A router may crash after receiving DNS TCP queries.

  Conditions: The symptom is observed on a router with “ip dns server” configured.

  Workaround: There is no workaround.

- CSCsx15370

  Symptoms: EIGRP commands may disappear from the interface configuration.

  Conditions: The symptom is observed on Cisco routers that are running Cisco IOS Release 12.4T and following an interface flap.

  Workaround: There is no workaround.

- CSCsx18860

  Symptoms: Traffic does not pass.

  Conditions: The symptom is observed with a Cisco VPN Acceleration Module 2+ (VAM2+) originating traffic and with process switching.

  Workaround: There is no workaround.

- CSCsx19184

  Symptoms: Cisco 2821 got bus error crash even though there was no configuration change or hardware change.

  Conditions: Happens while running an internal image with potential fix for CSCsv20948 and CSCsw44230.

  Workaround: There is no workaround.

- CSCsx19577

  Symptoms: The router is crashing while booting with the c3270-adventerprisek9-mz.124-22.T1.fc2 image.

  Conditions: The symptom is observed with the c3270-adventerprisek9-mz.124-22.T1.fc2 image.

  Workaround: There is no workaround.

- CSCsx20656

  Symptoms: There is traceback after using the **auto qos voip trust** command under frame-relay mode.

  Conditions: This issue is seen with a Cisco 7200 series router loaded with Cisco IOS Release 12.4(23.15)T2.

  Workaround: There is no workaround.

- CSCsx21482

  Symptoms: The following commands executed from the console result in a device reload: **write**, **copy running-config startup-config** or **show run**.

  Conditions: The symptom is observed when a large number of interfaces (200+) have been configured for RIPv6 and are active. Interfaces which are down will not contribute to the problem.

  Workaround: There is no workaround.

- CSCsx22101

  Symptoms: The call-forward night service will not trigger on CME when night service is active.

  Conditions: The symptom is observed when night service is activated and a call comes in to an extension where call-forward night service is configured.

  Workaround: There is no workaround.

- CSCsx23602

  Symptoms: Catalyst 6000 running modular Cisco IOS 12.2(33)SXH4 may crash with NAT configuration.

  Conditions: Occurs when running modular IOS with NAT deployment. Crash only happening in production, and NAT translation is required for crash to occur.

  Workaround: Run non-modular Cisco IOS Release 12.2(33)SXH4.

- CSCsx25880

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml.

- CSCsx29605

  Symptoms: QSIG-rose memory leak is seen with QSIG MWI feature enabled. The topology is:

  Avaya phones----Avaya PBX---QSIG----ISR----SIP-----IP Unity Voice Mail

  Conditions: The leak is observed per call during the following call scenario:

  Leave Message -> MWI ON -> Retrieve Message -> MWI OFF.

  Workaround: There is no workaround.

- CSCsx34297

  Symptoms: Watchdog reset seen with combination of NPEG1+PA-POS-1OC3/PA-POS-2OC3.

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

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

- CSCsx34703

  Symptoms: In certain corner cases, received BFD packets can fill up the input queue on the incoming interface eventually blocking packet reception on that interface.

  Conditions: The symptom is observed when BFD is enabled and BFD adjacency is established after bootup.

  Workaround: There is no workaround.

- CSCsx35306

  Symptoms: Router crashes at “t3e3_ec_safe_start_push”.

  Conditions: The crash is seen immediately after removing the channel-group of the PA-MC-2T3/E3-EC card.

  Workaround: There is no workaround.

- CSCsx41496

  Symptoms: When the fastethernet interface is up, the **reload** command takes the card to an empty state. You need to enter **resetcd** from the PXM to bring the card to an active state.

  Conditions: The symptom is observed when the fastethernet interface is connected to a Cisco 3750 router, a 2950 switch and an RPMXF card. The fastethernet interface should be up.

  Workaround: Enter **resetcd** from the PXM.

- CSCsx41624

  Symptoms: In a rare situation 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.

  Conditions: The symptom is observed when the SSLVPN process is waiting for HTTP REQUEST from a client on the port configured using **http-redirect <port no>** and never wakes up. This can happen because of an unexpected IPC message to SSLVPN process by another IOS process.

  Workaround: Remove **http-redirect**.

- CSCsx45429

  Symptoms: The GM crashes when trying to display VSA policy detail using the command **show pas vsa policy detail** and when traffic is being sent through the GM.

  Conditions: The symptom is observed when using the command **show pas vsa policy detail**. It may affect all recent software releases.

  Workaround: There is no workaround.

- CSCsx45923

  Symptoms: On a router that has a Virtual Tunnel Interface (VTI) IPSec configuration, an access control list (ACL) may be bypassed when there is an ACL on the tunnel interface. This happens only in the case where the physical interface (facing the IPSec peer) also has an ACL.

  Conditions: This symptom is observed when there is an ACL configured on the physical interface (facing the IPSec peer).

  Workaround: Apply the ACL on the protected LAN interface in the outbound direction, instead of on the tunnel interface

- CSCsx48272

  Symptoms: A router acting as an EasyVPN client may fail to build the IPSec tunnel and hang in the IPSEC_ACTIVE state, as shown in the **show crypto ipsec client ezvpn** command output.

  Conditions: It is not clear at this point what triggers this failure.

Workaround: There is no workaround.

- CSCsx48738

  Symptoms: Any queueing policy application on a tunnel interface, with a tunnel state change in parallel, may cause the router to crash.

  Conditions: The symptoms are observed with Cisco IOS Release 12.4(20)T2 and 12.4(24)T

  Workaround: If you need to unconfigure QoS on the tunnel, remove the policy first and then shutdown the tunnel. If you need to configure QoS on the tunnel, bring up the tunnel first and then apply QoS.

- CSCsx49555

  Symptoms: There may be a crash at OCE functions after disabling netflow by using the command **no ip flow ingress**.

  Conditions: The symptom occurs when both crypto and netflow configurations are applied.

  Workaround: Do not run crypto along with netflow.

- CSCsx51103

  Symptoms: Router crashes at an OCE function in crypto switching code.

  Conditions: The symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4(20)T, 12.4(22)T and 12.4(24)T. The following steps are used to generate the crash:

  1. Start VPN client and initiate connection.
  2. After successful connection, open DOS prompt.
  3. Start a trace route (tracert) to an internal IP OR start to an external IP.

  Workaround: There is no workaround.

- CSCsx51792

  Symptoms: The basic ping fails between two end-to-end ATM interfaces.

  Conditions: The symptoms are observed when two end-to-end ATM interfaces are configured. The ping fails.

  Workaround: There is no workaround.

- CSCsx55741

  Symptoms: Transit IPSec traffic is dropped on GM GETVPN. The following message is shown:

  ```
  %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
  destaddr=192.168.6.1, prot=50, spi=0xC39A071A(3281651482), srcaddr=192.168.6.2
  ```

  Conditions: The symptoms are observed under the following conditions:

  1. A Cisco 7200 series router in combination with VSA as HW-accelerator.
  2. GDOI policy defined to not perform double encryption.
  3. R1 connects to R2[GM], connects to R3[GM], connects to R4. (R2 and R3 are two group members of a GETVPN networks.) The GDOI policy is: Deny R1=>R4; Deny R4=>R1; Permit any any.

  Workaround: Permit double encryption with the following caveat: If transmitting ESP packets are near the IPSec path MTU then, after encapsulation into GETVPN IPSEC, they will be fragmented. The receiving side of the transit IPSec flow (e.g. R1 or R4 in above scenario) will have to reassemble these packets, which can lead to high CPU on the receiving end.

  This makes the workaround more or less applicable depending on the transiting traffic pattern.

- CSCsx57925

  Symptoms: A Cisco 2811 ISR may crash.

  Conditions: The symptom is observed on a Cisco 2811 ISR that is running Cisco IOS Release 12.4(20)T2 and with NAT NVI configured.

  Workaround: There is no workaround.

- CSCsx58009

  Symptoms: SAMI PPC crashes due to a SegV exception at the L2TP process.

  Conditions: The symptom is observed under the following conditions:

  1. L2TP communication down keeps more than 180 seconds between LAC and LNS.
  2. Crash will occur where the communication down happens after about 17 seconds from receiving the last L2TP hello.

  Workaround: Avoid sending L2TP hello at L2TP shutting down process by L2TP shutdown timer expiration. (For example, use **l2tp tunnel timeout no-session 0**. The command will teardown the session immediately when there is no session.)

- CSCsx59039

  Symptoms: Router crashes at SCCP SPI functions when handling events from STCAPP.

  Conditions: This is a corner case that occurs rarely. Only if STCAPP unregisters its SCCP device (forced by a DSP problem, in this case) while the corresponding voice-port is still active (having some internal event in the SCCP SPI queue to be processed after the unregistration), the crash can occur.

  Workaround: There is no workaround.

- CSCsx60891

  Symptoms: A numbered ACL with an object-group reference is not nvgened properly.

  Conditions: Global (numbered) ACL configuration mode does not support OG. (You can configure OG for numbered ACLs using sub-configuration (named) mode.) This issue applies only to numbered ACLs.

  Workaround: Use named ACLs in place of numbered ACLs.

- CSCsx63982

  Symptoms: A router configured for SNMP might unexpectedly crash with a bus error code.

  Conditions: This issue occurs when you query cSipCfgPeerTable of CISCO-SIP-UA-MIB. To be more specific, cSipCfgPeerPrivacy MIB object.

  Workaround: Do not poll cSipCfgPeerPrivacy MIB object.

- CSCsx68254

  Symptoms: Device will crash when loading the configuration with service policies with ACLs.

  Conditions: This is seen when more than 200 ACL filters are used in a service policy.

  Workaround: Remove unused ACLs in class-maps to get under the 200 limit. (The fix allows for 512 filters.)

- CSCsx73867

  Symptoms: A router that is running Cisco IOS Release 12.4(22)T and that is configured for L2L tunnels may intercept pass-through UDP 4500 packets destined to an internal client. Logged on the fault router is:

```
%CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
destaddr=x.x.x.x, prot=50, spi=0xDD8DEB2(232316594), srcaddr=y.y.y.y.
```

Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.4(22)T configured for IPSec. Internal IPsec client is natted on the router using NAT-T.

Workaround: There is no workaround.

- CSCsx74657

  Symptoms: Multiple issues are seen on multicast NAT. NAT is adding the number of dynamic entry statistics for every new multicast packet, even though there is already an existing NAT flow entry. This causes the number of dynamic entries to be inconsistent with the output from **show ip nat trans**. Also, dynamic NAT entries cannot be deleted with **clear ip nat trans ***. Finally, every fragmented multicast packet creates a separate NAT entry.

  Conditions: Occurs when **ip pim sparse-dense-mode** is configured on the interfaces with NAT overload.

  Workaround: There is no workaround.

- CSCsx75004

  Symptoms: In a Carriers Carrier, the CSC-PE router advertises wrong out-label. This causes the end-to-end LSP to be broken in the CSC network, and all traffic is dropped.

  This problem is observed by enabling the **show ip bgp label** command on CSC-CE. See "Out Label" of the route is "imp-null".

  Conditions: This condition is observed in routers that are running Cisco IOS Release 12.0(32)SY6.

  Workaround: Configure **neighbor** {*ip-address* | *peer- group-name*} **next-hop-self** on CSC-PE.

- CSCsx82690

  Symptoms: A voice gateway placing ISDN calls will exhibit a memory leak. The effects of this memory leak can be seen with the **show process memory** command. It shows that the amount of memory the ISDN process is holding continues to increase without being released.

  Conditions: The symptom is observed on a voice gateway that is processing ISDN calls on a PRI interface. Switchtype is set to be primary-QSIG and the calls that leak memory are QSIG-GF (connection-oriented calls) and not regular voice calls. Such calls are typically used when implementing supplementary services such as MWI.

  Workaround: There is no workaround.

- CSCsx96381

  Symptoms: A video conference device makes a video call to a TDM Conference Station through an H320 gateway. When the call is placed, only the primary channel goes up and the H320 gateway does not proceed with secondary channels.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsy09101

  Symptoms: Cisco Configuration Professional (CCP) is unable to load signatures from the router. IOS-IPS signatures cannot be viewed or modified using CCP.

  Conditions: The symptom occurs when using CCP to manage IPS5.0 in routers that are running Cisco IOS Release 12.4(20)T2, 12.4(24)T and 12.4(22)T1.

  Workaround: There is no workaround from CCP. Use CLI to view or modify IPS signatures.

- CSCsy15227

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

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:

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

- CSCsy15468

  Symptoms: Crash keyserver reloads.

  Conditions: The symptom is observed if test case 1 in TBAR sanity regression on the VSA is configured and then unconfigured. When configuring the second one, the keyserver crashes.

  Workaround: There is no workaround.

- CSCsy16092

  Symptoms: A Cisco router that is running Cisco IOS or IOS XE may unexpectedly reload due to watchdog timeout when there is a negotiation problem between crypto peers.

  The following error will appear repeatedly in the log leading up to the crash:

  ```
  ISAKMP: encryption... What? 0?
  ```
  Conditions: The device must have “debug crypto isakmp” enabled.

  Workaround: Turn off the debug

- CSCsy16220

  Symptoms: A switch may reload with messages on both the RP and SP similar to:

  ```
  %CPU_MONITOR-2-NOT_RUNNING: CPU_MONITOR messages have not been sent for 30 seconds
  ```
  Conditions: The symptom is observed with SNMP polling configured for SNMP MIB:

  ```
  ceemEventMapEntry, oid 1.3.6.1.4.1.9.10.91.1.1.1.1
  ```
  This crash will only occur on modular IOS.

  Workaround: Disable SNMP polling of SNMP MIB:

  ```
  ceemEventMapEntry, oid 1.3.6.1.4.1.9.10.91.1.1.1.1
  ```
- CSCsy22920

  Symptoms: A router crashes at mripv6_mode_entry when the authentication key is configured to be equal to 64 bytes.

  Conditions: The symptom is observed on a router that is running the c7200-adventerprisek9-mz.124-24.6.T image.

  Workaround: Configure an authentication key of less than 64 bytes.

- CSCsy24676

  Symptoms: On occasion, a false positive is returned on a file system failure. File operation is deemed successful when, in fact, it has failed.

  Conditions: This problem occurs when the file system device returns an error and the code follows the path in the file system buffer cache where the error is masked and converted to a success code. This problem is likely to show up if there is a device error during the write. The device error may be due to bad media or an OIR (although it is very unlikely during an OIR).

  Workaround: There is no workaround.

Further Problem Description: This is possible during any file system operation where a file system device is unable to complete the operation and an error is returned. This error is not passed down to the file system stack but is converted to a success code. Other clients which are dependent on previous file system operations fail on successive file system calls and possibly result in a crash.

- CSCsy27394

  Symptoms: Users who can execute a **show ip interface** command can see that an LI tap is in progress.

  Conditions: No specific conditions are necessary to trigger this problem.

  Workaround: There is no workaround.

- CSCsy28758

  Symptoms: HLog softkey stops working.

  Conditions: The symptom is observed under the following conditions:

  1. When logging into an EM profile where the user was logged out from the hunt group.
  2. This is to be done on a phone where an EM profile was previously logged in, which was also logged into the huntgroup.

  Workaround: Log in with the EM profile on the phone that was used to log out the huntgroup.

- CSCsy29828

  Symptoms: A Cisco router may reload due to a bus error. The error indicates trying to read address 0x0b0d0b**, where ** is around 29.

  Conditions: This has been experienced on a Cisco 2800 series router running Cisco IOS Release 12.4(24)T. The router must be configured with NAT, and SIP traffic is passed through the NAT router.

  Workaround: Enter the following commands:

  * **no ip nat service sip tcp port 5060**
  * **no ip nat service sip udp port 5060**

  Or

  * **ip nat translation timeout never**

- CSCsy31365

  Symptoms: Memory leak of 24-bytes can occur when a transcoding call is disconnected.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(24.6)T and is seen while shutting down the DSPfarm profile when the transcoding call is active in IPIPGW.

  Workaround: There is no workaround.

- CSCsy55800

  Symptoms: OSPF route gets stuck in the RIB.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(15)T and later. It is seen if a valid LSA for the same network exists but is filtered via a route-map.

  Workaround: Using the command **clear ip route X.X.X.X** will temporarily fix the issue, but the problem will reoccur each time the permitted route is withdrawn.

- CSCsy58984

  Symptoms: A device that is running Cisco IOS Release 12.4(24)T reloads when editing ACL with an object group.

  Conditions: The symptom is observed on a Cisco 3845 and 2800 series router that is running Cisco IOS Release 12.4(24)T and 12.4(24.6)T2.

Workaround: Avoid using “range” in any of the object groups (either direct or nested) and containing a group of objects which use a range of IP addresses.

- CSCsy61209

  Symptoms: An IP-to-IP gateway (IPIPGW), also called CUBE, is adding an incorrect token in the H225 connect message.

  Conditions: The symptom is observed on an IPIPGW running Cisco IOS Release 12.4(20)T1, with talking H323 signaling protocol on both sides with security enabled.

  Workaround: There is no workaround.

- CSCsy70619

  Symptoms: A router may crash when multipath is enabled and when the MR is registered with two or more of its roaming interfaces.

  Conditions: The symptom is observed when using the **no ip mobile router-service roam** command on any one of the MRs roaming interfaces.

  Workaround: There is no workaround.

- CSCsy71258

  Symptoms: Unable to boot a Cisco 850 series router using Cisco IOS Release 12.4(15)T9.

  Conditions: The symptom is observed on a Cisco 850 series router with 64MB of dram. The image requires more dram to boot.

  Workaround: There is no workaround.

- CSCsy79138

  Symptoms: Due to the fix of CSCsi26296, sometimes IPSec VPN tunnels disconnect, and the tunnel will not recover until:

  1. rekey starts due to the expiry of the IPSec SA OR
  2. manually clearing the crypto sessions on the peers

  Conditions: Routers are affected after Cisco IOS Releases 12.4(11)T3.

  Workaround:

  1. Use lower IPSec lifetimes to trigger rekeying more frequently, but this causes increased CPU utilization.
  2. Set up Embedded Event Manager to monitor certain syslog messages and trigger the “clear crypto session”.

  Further Problem Description: The feature “Invalid SPI Recovery” should normally be triggered, but that is not happening so the routers get stuck at the failed state.

- CSCsy79176

  Symptoms: Need to disable CEF to pass IP traffic. With CEF enabled, traffic fails to pass.

  Conditions: The symptom is observed on a Cisco 2801 and 2811 router that is running the ipvoicek9-mz.124-23_15_PI10 image.

  Workaround: Disable CEF OR shut/unshut the interface with incomplete adjacency (using the **show adjacency** command).

- CSCsy84474

  Symptoms: In an H323 IP-to-IP Gateway (IPIPGW), during call setup when the OLC-ACK is received after the connect message, the call is not completed and the return OLC-ACK is not forwarded by the IPIPGW. The issue is sporadic and does not occur all the time.

Conditions: This has been observed on a IPIPGW running Cisco IOS Release 12.4(20)T1-ES, having an H323 on both sides of the gateway. This only happens when the connect message is received before OLC-ACK exchange between the parties is complete.

Workaround: There is no workaround.

- CSCsy95484

  Symptoms: Ping fails from gen to ref.

  Conditions: The symptom is observed when the router is loaded with Cisco IOS Release 12.4(24.6)T5.

  Workaround: Perform a **shut** and **no shut** on the VLAN interface and the ping passes.

- CSCsy97506

  Symptoms:

  Case 1: All NAT multicast data packets are processed by software.

  Case 2. Spurious memory access occurs.

  Conditions:

  Case 1. NAT with static port entry, or dynamic overload configuration.

  Case 2. Configure **ip nat dynamic nat** rule with an undefined NAT pool.

  Workaround:

  Case 1: Configure NAT as static entry without port, or dynamic non-overload.

  Case 2: Configure with defined pool.

Resolved Caveats—Cisco IOS Release 12.4(20)T2

Cisco IOS Release 12.4(20)T2 is a rebuild release for Cisco IOS Release 12.4(20)T. The caveats in this section are resolved in Cisco IOS Release 12.4(20)T2 but may be open in previous Cisco IOS releases.

- CSCeg49153

  Symptoms: It may take a long time for the IPSec router to detect that the CA server is down while trying to reach it for CRL retrieval.

  Conditions: The symptom is observed on a LAN-to-LAN IPSec tunnel between two routers, where one router is configured for CRL checking.

  Workaround: The situation may be slightly improved by lowering the “tcp synwait” value, for example:

  ip tcp synwait-time 5

- CSCeg87070

  Symptoms: A Cisco 10000 crashes at igmp-process:

  ```
  Cisco IOS Software, 10000 Software (C10K2-P11-M), Version 12.3(7)XI2b, RELEASE
  SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c)
  1986-2005 by Cisco Systems, Inc. Compiled Sat 08-Jan-05 16:25 by <software engineer>
  ROM: System Bootstrap, Version 12.0(20020314:211744) [REL-pulsar_sx.ios- rommon 112],
  DEVELOPMENT SOFTWARE
  r-pa068 uptime is 19 hours, 58 minutes System returned to ROM by RPR switchover at
  19:03:47 MET Mon Jan 24 2005 System restarted at 19:07:22 MET Mon Jan 24 2005 System
  image file is "disk0:c10k2-p11-mz.123-7.XI2b"
  ```

  Conditions: This symptom is observed during 7xi2b monitoring.

Workaround: There is no workaround.

- CSCek32744

  Symptoms: The vlan-id is not propagated in the NAS Port ID field when the PPPoE over VLAN call is up.

  Conditions: The symptom is observed when using both configurations (main interface and sub-interface) for PPPoE over VLAN. The NAS Port ID value shows correctly while using the sub-interface configuration but incorrectly when using the main interface. The main interface used for PPPoE over VLAN is shown below:

  interface Ethernet1/0
  no ip address
  vlan-id dot1q 4
  pppoe enable group global
  exit-vlan-config

  The expected NAS Port ID is 1/0/0/4, but 1/0/0/0 is received.

  Workaround: There is no workaround.

  Further Problem Description: This will impact AAA because this information should be updated by PPP to AAA.

- CSCek72156

  Symptoms: Router might crash while performing nonvolatile generation (NVGEN) with compiled standard ACLs.

  Conditions: Occurs only with compiled standard ACLs. Does not occur without compiled ACLs.

  Workaround: There is no workaround.

- CSCek75694

  Symptoms: A router that is running Cisco IOS 12.4T may reload unexpectedly.

  Conditions: Occurs when BFD is configured and active.

  Workaround: Disable the BFD feature.

- CSCek77424

  Symptoms: A Cisco router that is running Cisco IOS Release 12.4(13b) might unexpectedly reload with a bus error.

  Conditions: This symptom happens during normal operation with NAT configured.

  Workaround: There is no workaround.

- CSCsc78999

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

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

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

- CSCsd35958

  Symptoms: A Cisco 7304 that is configured with an NPE-G100 processor and ATM VCs may reload unexpectedly.

  Conditions: This symptom is observed when a hierarchical policy on an ATM VC has the **shape average** command enabled.

  Workaround: Do not use a hierarchical policy on an ATM VC.

- CSCse26506

  Symptoms: When you perform an OIR of an ATM line card, a CPUHOG condition may occur in the "BGP Event" process.

  Conditions: This symptom is observed when the ATM line card is configured with about 15,000 /32 routes.

  Workaround: There is no workaround.

  Further Problem Description: The ATM line card connects to about 15,000 different gateways, each of which is covered by its own /32 route. In addition, there is a less specific route that covers everything. The symptom occurs when BGP attempts to remove a large number of these tracked entries without suspending any.

- CSCsg39977

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

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

  Workaround: There is no workaround.

- CSCsg44748

  Symptoms: A Cisco IOS VoIP gateway configured for IPIPGW (CUBE) functionality may crash.

  Conditions: A gateway configured for IPIPGW functionality with the command **allow-connections** under **voice service voip** under rare conditions will crash while processing VoIP calls.

  This has been found to occur in some scenarios where a single voip call loops (meaning the call is from the IPIPGW back to the same IPIPGW) through the IPIPGW.

  When this occurs, the following error message may be noticed:

  ```
  %SYS-6-STACKLOW: Stack for level Network interfaces running low, 0/9000
  ```

  Workaround: Track down the source of the call looping and correct the problem there.

  The other possible workaround is to introduce another termination point in the RTP packet flow beside the IPIPGW. For example, if interworking with Cisco Unified Communications Manager (Callmanager) a MTP resource may be used to prevent this loop.

- CSCsg45637

  Symptoms: A traceback may be generated when the router accesses the "bgp_vpnv4_lookup_prefix" function.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP VPNv4.

  Workaround: There is no workaround.

- CSCsg92618

  Symptoms: Entering the **crypto key zeroize rsa** command causes a traceback.

  Conditions: This symptom is observed in router loaded with the Cisco IOS software image.

  Workaround: There is no workaround.

- CSCsi17158

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

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

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

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

  line vty 0 4 transport input telnet end

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

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

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

  http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

- CSCsi35544

  Symptoms: A router may reload with the message "Unexpected exception to CPU."

  Conditions: The symptom is observed when EzVPN remote using client mode is configured on the router. It is seen when an IP address is being removed from one of the EzVPN inside interfaces while having active NAT translations.

  Workaround: There is no workaround.

- CSCsi68795

  Symptoms: A PE that is part of a confederation and that has received a VPNv4 prefix from an internal and an external confederation peer, may assign a local label to the prefix despite the fact that the prefix is not local to this PE and that the PE is not changing the BGP next-hop.

  Conditions: The symptoms are observed when receiving the prefix via two paths from confederation peers.

  Workaround: There is no workaround.

  Further Problem Description: Whether or not the PE will chose to allocate a local label depends on the order that the multiple paths for this VPNv4 prefix are learned. The immediate impact is that the local label allocated takes up memory in the router as the router will populate the LFIB with the labels.

- CSCsi99449

  Symptoms: A traceback is seen.

Conditions: This symptom is observed when the WLAN feature of NAT is configured and when the host with the static IP address tries to contact any host connected to the outside interface of the NAT.

Workaround: There is no workaround.

- CSCsj33299

  Symptoms: When performing SSLVPN stress tests, thousands of tracebacks are seen on the console. Sometimes there are so many tracebacks, it is hard to get console access. In addition, after many of these tracebacks are seen, the SSLVPN traffic rate that is maintained by the router drops significantly.

  Conditions: This symptom is observed when performing SSLVPN stress tests.

  Workaround: There is no workaround.

- CSCsj34557

  Symptoms: Router displays following error message and reloads:

```
Jun 18 06:12:23.008: event flooding: code 10 arg0 0 arg1 0 arg2 0
%SYS-3-OVERRUN: Block overrun at E5D8310 (red zone 00000000) -Traceback= 0x6080CEB0
0x60982108 0x60982EC0 0x6098511C 0x609853BC %SYS-6-MTRACE: mallocfree: addr, pc
662B5B1C,608A6F3C 0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 662B5B1C,608A6F3C
0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 %SYS-6-MTRACE: mallocfree: addr, pc
662B5B1C,608A6F3C 0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 662B5B1C,608A6F3C
0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 %SYS-6-BLKINFO: Corrupted redzone blk
E5D8310, words 6088, alloc 61FE2638, InUse, dealloc 80000000, rfcnt 1 -Traceback=
0x6080CEB0 0x609681D4 0x6098211C 0x60982EC0 0x6098511C 0x609853BC %SYS-6-MEMDUMP:
0xE5D8310: 0xAB1234CD 0xFFFE0000 0x0 0x63894208 %SYS-6-MEMDUMP: 0xE5D8320: 0x61FE2638
0xE5DB2D0 0xE5D8144 0x800017C8 %SYS-6-MEMDUMP: 0xE5D8330: 0x1 0x0 0x1 0x64B53478
%Software-forced reload
```

  Conditions: Occurred on a Cisco 7200 that was running the c7200-ik9s-mz.124-7a.bin image.

  Workaround: There is no workaround.

- CSCsj36031

  Symptoms: The configuration for "xconnect" may not be accepted.

  Conditions: Problem seen only when the existing "xconnect" configuration is removed from ATM PVC with “encap aal0” and then attached to the same ATM PVC.

  Workaround: Remove the ATM PVC and reconfigure again with aal0 encapsulation and "xconnect".

- CSCsj36133

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

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

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

- CSCsj56281

  Symptoms: An inherited peer policy does not work.

  Conditions: This symptom is observed after a router reload.

  Workaround: There is no workaround.

- CSCsj84572

  Symptoms: The **l2 vfi ...** configuration command is rejected by the parser as an ambiguous command.

  Conditions: The symptom is observed when the router is in configuration mode and a command beginning with **l2 vfi** is entered.

  Workaround: There is no workaround.

- CSCsj97952

  Description: A large file (typically of sizes greater than 60 MB, which we took as a reference to reproduce the problem) that is copied using Windows networking (PC-to-PC drag and drop on a shared drive) across a network can cause unexpected latency for traffic in different QoS classes when the access is via a Cisco 3845 with an NM-1A-OC3-POM interface.

  Symptoms: When a large file is copied using Windows file transfer (best- effort traffic), the priority class traffic gets delayed and sees high latency values (at the maximum, the latency can reach 100 ms with average hovering around 60 ms).

  Conditions:

  - Hardware Configuration: This bug is seen when an NM-1A-OC3-POM card is used for passing the traffic on a low-bandwidth PVC (1-Mbps PVC was used while testing).
  - Software Configuration: Configure priority EF traffic stream with 30 percent of 1 Mbps reserved and the rest of the bandwidth set aside for best- effort traffic.
  - Network Conditions: This symptom occurs when a low-bandwidth PVC is configured (less than 10 Mbps) and is due to the bursty nature of best-effort traffic ONLY.

  Workaround: This observation is made only when the input best-effort traffic is bursty in nature. Regularized best-effort traffic flow does not seem to affect other priority traffic classes. To eliminate the symptoms, apply input policing to rate-limit best-effort traffic.

- CSCsk41593

  Symptoms: The following error occurs when a ping packet is sent or received:

  ```
  PAK_SUBBLOCK_ALREADY: 2 -Process= "IP Input"
  ```

  Conditions: Occurs when large ping packets (greater than 1500 bytes) are sent to back-to-back cellular interfaces with GRE tunneling enabled.

  Workaround: Disable the **ip virtual-reassembly** command on the cellular interface.

- CSCsk98751

  Symptoms: A router may crash after the **mpls traffic-eng backup-path tunnel** command is issued.

  Conditions: The symptom is observed when a backup tunnel is configured on PLR, which is a midpoint router for a protected primary tunnel.

  Workaround: There is no workaround.

- CSCsk99687

  Symptoms: A router may crash.

  Conditions: The symptoms are very rare, but if it occurs, it will be seen during ISSU runversion.

  Workaround: There is no workaround.

- CSCsl00472

  Symptoms: A Cisco router unexpectedly reloads with memory corruption after showing multiple "%SYS-2-INPUT_GETBUF: Bad getbuffer" messages.

Conditions: This symptom occurs during normal operation.

Workaround: There is no workaround.

- CSCsl16001

  Symptoms: Booting from compactflash or usbflash or writing kernel dumper takes a long time.

  Conditions: This symptom occurs in Cisco IOS Releases 12.4(15r)XZ02, 12.4 (21.04)T, and 12.2(32.08.11)SX188.

  Workaround: There is no workaround.

- CSCsl49628

  Symptoms: When a VPN routing/forwarding (VRF) is deleted through the CLI, the VRF deletion never completes on the standby RP, and the VRF cannot be reconfigured at a later time.

  Conditions: This symptom is observed when BGP is enabled on the router.

  Workaround: There is no workaround.

- CSCsl92316

  Symptoms: Router may experience mwheel CPUHOG condition.

  Conditions: This condition is observed on Cisco router while clearing all L2TP sessions when there are more than 2500 sessions with multicast traffic flowing on the sessions.

  Workaround: There is no workaround.

- CSCsk64158

  Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml.

- CSCsm01389

  Symptoms: Crash occurs after clearing auto-tunnel backup by issuing the **clear mpls traf-eng auto-tunnel backup** command.

  Conditions: Occurs with SSO and traffic engineering (TE) auto-tunnel feature enabled.

  Workaround: There is no workaround.

  Further Problem Description: Crash was seen on the Active SP after issuing the **clear mpls tra auto-tunnel primary** command followed by the **clear mpls tra auto-tunnel backup** command. This crash could happen with or without a SSO switchover before issuing those commands.

- CSCsm03452

  Symptoms: A Cisco AS5850 that is configured as a SIP gateway may crash unexpectedly when running a high volume of SIP calls.

  Conditions: This symptom is observed on the Cisco AS5850.

  Workaround: There is no workaround.

- CSCsm34002

  Symptoms: CPU utilization goes to 99 percent. It stays there for few seconds and then reduces to around 50 percent, and then to 2 percent. After few seconds, CPU utilization reaches 99 percent, and this cycle continues.

  ```
  Router# show proce cpu sorted

  Conditions: This symptom is observed when around 2000 PPPOE sessions are initiated.
  ```

  Workaround: There is no workaround.

- CSCsm50741

  Symptoms: When a non-DC router is removed from a DC enabled area and the area becomes DC enabled, some of the LSAs are not refreshed correctly with DoNotAge (DNA) bits set. Crash may happen when customer deploys iptivia probes in the network. Fixed in CRS.

  Conditions: The symptom is observed when a router without DC capability is removed from a DC enabled area.

  Workaround: Use the **clear ip ospf** command.

- CSCsm54614

  Symptoms: A service-policy may not be removed from a frame relay map-class when the FR-DLCI's circuit is reduced to less than the configured bandwidth of the policy-map.

  Conditions: The symptoms are observed under the following conditions:

  - A policy with an absolute bandwidth is configured and then configured as a service-policy in a Frame Relay map-class.
  - The FR-DLCI's circuit is reduced to less than the configured bandwidth of the policy map.

  Workaround: Manually remove the service-policy from the map-class.

- CSCsm55817

  Symptoms: When configuring ATM PVCs, under the PVC syntax you can provide a handle to describe the PVC. If this handle starts with "00" (zero zero) then the command will fail.

  Conditions: The symptom is observed when configuring ATM PVCs and where the PVC handle starts with "00".

  Workaround: Do not use handles that start with "00".

- CSCsm69762

  Symptoms: 802.1X supplicants are sometimes not authenticated on the network.

  Conditions: This symptom is observed under normal operation.

  Workaround: Shut down and bring back up the interface to which the supplicant is attached.

- CSCsm83996

  Symptoms: GM encrypts packets that match GMACL deny.

  Conditions: This symptom is observed when the GMACL is configured on the highest priority crypto map.

  Workaround: Configure the GMACL on a lesser priority crypto map.

- CSCsm96785

  Symptoms: You may observe a problem which the OSPF neighbor is down after switch-over in spite of using OSPF Non-Stop Forwarding (NSF).

Conditions: This occurs with the following conditions:

- "nsf cisco" is only affected. If "nsf ietf", this problem does not occur.
- You may observe this problem if the OSPF interface is "point-to-multipoint non-broadcast" or "point-to-multipoint". If the interface is "broadcast", this problem does not occur.
- When this problem occurs after switch-over, DBD packet may not be exchanged between two neighbors. And the neighbor is down in spite of NSF.

Workaround: Change the OSPF config to "nsf ietf" and change the OSPF interface to "broadcast".

- CSCso15740

  Symptoms: The "set metric" clause in the continue route-map sequence is not setting metric correctly in some particular conditions. This is also applicable in case where the nexthop setting is done via route-map with a continue clause.

  Conditions: The symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(32)SY4. This is platform independent. This symptom occurs if the route-map has a continue clause and the match condition does not allow the continue clause to be executed. The following route-map sequence which has to be executed will not execute properly if the metric or nexthop of the prefix are to be modified via the route-map.

  Workaround: Avoid using “continue” in a route-map and modifying metric or nexthop via the following route-map sequence.

- CSCso21463

  Symptoms: A one-way voice issue is seen when making a transcoded transfer call with an H.323 endpoint.

  Conditions: A one-way voice issue is observed when DSP farm resources are controlled by CCM and the transcode profile has g711alaw and g729 codecs, but no g711ulaw, configured on the DSP farm router. The checkbox for MTP required is checked under the H.323 gateway configuration page.

  Workaround: Add g711ulaw in the transcode profile.

- CSCso33848

  Symptoms: PPP call may fail with stack group configured.

  Conditions: Failure will happen only when call initiated to stack group member.

  Workaround: Initiate PPP call directly to stack group master.

- CSCso39597

  Symptoms: The redundant RP in a dual-RP router may crash in certain cases when BGP is unconfigured and then an SSO is performed.

  Conditions: The symptom is observed on a redundant RP in a dual-RP router that is running Cisco IOS Release 12.2(33)XN with BGP VPNv4 configuration. It is observed when BGP is unconfigured first and then an SSO is performed.

  Workaround: Avoid unconfiguring BGP prior to an SSO.

  Further Problem Description: The problem is platform independent. After the reset, the redundant RP is able to function normally.

- CSCso52598

  Symptoms: The router may crash after the **no interface ethernet 0/0.1** command is entered.

  Conditions: It could happen on a router with more than 4000 dynamic ARP entries.

  Workaround: Do not execute the **no interface ethernet 0/0.1** command.

- CSCso54167

  Symptoms: BGP peers are stuck with table versions of 0. BGP peers do not announce any routes to neighbors.

  Conditions: Whenever the interfaces flap with online insertion and removal (OIR) multiple times, all of the BGP peers using such interfaces for peering connections encounter this issue.

  Workaround: Delete and reconfigure the neighbor.

- CSCso57886

  Symptoms: A Cisco IOS device may crash with a data bus error exception and stack trace PC = 0xA0000100.

  Conditions: Device is running normal production traffic. Presence of malformed punted RP packets in this network caused the issue.

  Workaround: There is no workaround.

- CSCso67195

  Symptoms: Router may crash due to memory corruption:

  ```
  *Apr 7 12:32:14: %SEC-6-IPACCESSLOGRP: list 111 denied pim 0.0.0.0 -> <removed>, 1
  packet
  *Apr 7 12:32:29: %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk
  680A5374 data 680A79A4 chunkmagic FFFFFFFF chunk_freemagic 0 - Process= "Mwheel
  Process", ipl= 0, pid= 274, -Traceback= 0x6169C450 0x60102E78 0x601031E4 0x61D418E4
  0x61D4230C 0x61CF1A48 0x61D1280C 0x61D05FE4 0x61D0E9FC
  chunk_diagnose, code = 1
  chunk name is PIM JP GroupQ
  ```

  Conditions: This symptom occurs when PIM is enabled on an interface and access-list logging is enabled.

  ip pim sparse-dense-mode

  access-list 98 deny any log

  Workaround: Remove access-list logging.

- CSCsq05099

  Symptoms: User can only configure a maximum of 500 SWMTP sessions per profile.

  Conditions: This symptom is observed when using SWMTP.

  Workaround: Configure multiple SWMTP profiles.

- CSCsq13938

  Symptoms: In Cisco IOS software that is running the Border Gateway Protocol (BGP), the router may reload if BGP **show** commands are executed while the BGP configuration is being removed.

  Conditions: This problem may happen only if the BGP **show** command is started and suspended by auto-more before the BGP-related configuration is removed, and if the BGP **show** command is continued (for example by pressing the SPACE bar) after the configuration has been removed. This bug affects BGP **show** commands related to VPNv4 address family. In each case the problem only happens if the deconfiguration removes objects that are being utilized by the **show** command. Removing unrelated BGP configuration has no effect.

  This bug is specific to MPLS-VPN scenarios (CSCsj22187 fixes this issue for other address-families).

  Workaround: Terminate any paused BGP **show** commands before beginning operations to remove BGP-related configuration. Pressing "q" to abort suspended show commands, rather SPACE to continue them, may avoid problems in some scenarios.

- CSCsq18856

  Symptoms: Packets are not being switched by Cisco Express Forwarding (CEF).

  Conditions: This issue is seen on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsq19957

  Symptoms: A numbered access-group does not match traffic when configured under a class-map unless another matching criteria is added to the same class-map, which must be a non-numbered access-group match statement.

  Conditions: This has been observed for Gigabit ethernet on an NPE-G1, frame-relay encapsulated serial interface, and POS interfaces on a NPE-G2.

  Workaround:

  1. Add another match criteria under the same class, which has to be a non-numbered access-group such as **match ip dscp** or **match access-group<name>**. This triggers the numbered access-group to start matching traffic correctly.

  2. Have only one class defined plus class class-default under the policy-map, and it will classify traffic correctly.

- CSCsq22106

  Symptoms: All CAS voice calls fail on a Cisco AS5850. This failure is not seen on PRI calls.

  Conditions: This symptom is observed for CAS calls but not for PRI calls.

  Workaround: There is no workaround.

- CSCsq23391

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

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

  Workaround: There is no workaround.

- CSCsq29052

  Symptoms: Packets are not forwarded out from a point-to-point (P2P) interface.

  Conditions: The symptom is observed with CEF enabled and when the P2P interface is changed from an “ip unnumbered” configuration to another interface.

  Workaround: There is no workaround.

- CSCsq29139

  Symptoms: When IPv6 prefix delegation receives periodic RENEW message from a client, it may incorrectly bind the corresponding prefix for another client.

  Conditions: The symptom is observed when IPv6 prefix delegation assigns a prefix to a client that is connected via a virtual access interface.

  Workaround: There is no workaround.

- CSCsq33509

  Symptoms: Traceback@%SCHED-3-STUCKMTMR, Sleep with expired managed timer is seen while testing with CA servers.

  Conditions: The symptom is observed when running Cisco IOS Release 12.4 (19.18)T2.

  Workaround: There is no workaround.

- CSCsq36135

  Symptoms: A Cisco 3845 router may crash.

  Conditions: The symptom is observed when an SIP TNP phone with MWI configuration tries to register with the CME.

  Workaround: There is no workaround.

- CSCsq36269

  Symptoms: Packets being sent towards a Cisco 7200 that are group domain of interpretation (GDOI) encapsulated but which in fact the router wants to send out through the same interface (due to a routing problem) will not leave the router with the TTL decreased by one, but increased by one.

  As it is likely that the upstream router will send the packet again to the GDOI endpoint this will lead to a never-stopping flow of packets that will overwhelm the router.

  Conditions: Occurs when using GDOI on a Cisco 7200 and having a routing issue where the upstream router forwards packets towards the GDOI router, but the GDOI router wants to send the same traffic towards the upstream router.

  Workaround: There is no workaround.

- CSCsq37520

  Symptoms: A crash is seen when a child policy-map is added to a policy-map that is attached to a large number (1000s) of interfaces.

  Conditions: This symptom occurs when any configuration change results in the creation of 1000s of QoS queues at once.

  Workaround: Remove the policy-map from all interfaces prior to modification.

- CSCsq40600

  Symptoms: When 802.1X is configured on the WAN interface of a Cisco 871, none of the “Spouse & Kids” related policy configuration works. In fact, there is no access control applied on the port based on 802.1X authentication.

  Conditions: This symptom happens only on the WAN interface of the Cisco 871 platform.

  Workaround: There is no workaround for this because 802.1X is not supported on the WAN interface of the Cisco 871 and therefore should not be configured on this interface.

- CSCsq41361

  Symptoms: When the PIX initiates a phase 2 rekey, it sends the QM1 and the router responds with QM2 and immediately after that it sends IKE delete notify for the previous inbound SPI before receiving the QM3 from the PIX. The PIX after that sends the QM3 and the tunnel is rekeyed, but this causes the VPN tunnel to flap a bit and then PIX drops all TCP connections associated with that VPN tunnel.

  Conditions: Occurs when PIX initiates a phase 2 rekey.

  Workaround: There is no workaround.

- CSCsq42246

  Symptoms: Router crashes while reloading the satellite network module.

  Conditions: Occurs on a router running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsq44792

  Symptoms: Per session queuing does not work with PPPoE session.

Conditions: Occurs on a Cisco router configured for Mobile Ad Hoc Networks (MANET).

Workaround: There is no workaround.

- CSCsq46336

  Symptoms: Radio transmissions from LMR voice ports to PMCs may intermittently drop packets in the router.

  Conditions: The symptom is seen where multiple PMC users monitoring the same stream cause more than three simultaneous RTP streams to be present on the LMR router.

  Workaround: If customer is running PMC, turn off the keepalive on the PMCs.

- CSCsq50977

  Symptoms: Trimble Palisade NTP Synchronization Driver feature does not work.

  Conditions: Occurs on a Cisco 7200 NPE-G2 running Cisco IOS Release 12.4(15)T3 and Cisco IOS Release 12.4(15)T5. Issue is not seen on NPE-400 running 12.4(15)T3 and Cisco IOS Release 12.4(15)T5.

  Workaround: There is no workaround.

- CSCsq51158

  Symptoms: The signal of a Cisco 851w router may fluctuate.

  Conditions: This symptom applies to different environments where multipath is more of an issue.

  Workaround: There is no workaround.

  Further Problem Description: A spectrum analyzer shows that the router has a signal of -60 (+/- 10) Db and that it stays at that level for about 7 to 10 seconds. It then drops by 40 Db for 7 to 10 seconds before it restores itself to its original level.

- CSCsq57731

  Symptoms: A router that is configured with QoS + Firewall may crash while the **service-policy** command is unconfigured from a tunnel interface.

  Conditions: This symptom is observed when a zone-base firewall is configured along with QoS and when an attempt is made to remove the QoS **service- policy** command from a GRE tunnel interface.

  Workaround: There is no workaround.

- CSCsq70534

  Symptoms: A router crashes because of a block overrun (overwriting the memory block).

  Conditions: This symptom is observed only when templates are exported in the export packet, which is used in only version 9 of exporting.

  Workaround: Version 5 could be used for exporting.

- CSCsq75787

  Symptoms: Cannot enable AutoQoS on ATM subinterface.

  Conditions: This happens on a Cisco 3800 router running Cisco IOS Release 12.4(15)T06.

  Workaround: There is no workaround.

- CSCsq78956

  Symptoms: Memory tracebacks and errors occur.

  Conditions: Occurs only when using IKE in Cisco IOS Release 12.2SXH. May also occur in other Cisco IOS releases.

Workaround: There is no workaround.

- CSCsq83501

  Symptoms: Router crashes while configuring more than 256 channel-groups in PA-MC-2T3-EC.

  Conditions: The crash is seen after configuring more than 256 channel-groups in PA-MC-2T3-EC.

  Workaround: Do not configure more than 256 channel-groups.

- CSCsq87204

  Symptoms: A router may reload due to a crash after configuring the **no multi-path** command or the **shut** command.

  Conditions: This symptom occurs when the router is configured with Mobile IP, Mobile Router, and the **multi-path** command on Cisco IOS Release 12.4(9)T.

  Workaround: There is no workaround.

- CSCsq92019

  Symptoms: An SCCP phone cannot act as a conferencing controller.

  Conditions: This symptom is specific to a customer test setup where there is NAT back-to-back. NAT segmented code synchronization fails when NAT is back-to-back.

  Workaround: Configure the **no ip nat service skinny tcp port 2000** command.

- CSCsq92440

  Symptoms: A router may crash when continuously executing the **show ip mroute count | incl groups** command with large number of mroutes.

  Conditions: The symptom is observed only when unconfiguring a large number of static joins at a time or unconfiguring the class-map having large number of groups and executing the **show ip mroute count | incl groups** command multiple times continuously. (Unconfiguration/configuration of a large number of static joins can be done only by using a class-map.)

  Workaround: Do not check **show ip mroute count | incl groups** continuously when unconfiguring or configuring a large number of mroutes.

- CSCsq93004

  Symptoms: Removal of a subinterface may cause memory corruption or a crash. The symptoms are unpredictable.

  Conditions: The symptoms are rare and will be observed only if a subinterface is configured for **mpls traffic-eng auto-tunnel primary use** and the subinterface is later removed from the configuration.

  Workaround: Do not remove subinterfaces.

- CSCsq93508

  Symptoms: When onboard hardware crypto is enabled and if an SSLVPN AnyConnect tunnel is brought up, tracebacks are continuously seen and no traffic will go through the tunnel.

  Conditions: The symptom is observed with hardware crypto enabled on a Cisco 1800 series router.

  Workaround: Enable software crypto.

  Further Problem Description: The issue is seen on an 1800 platform because other ISR routers do not handle SSL with a hardware engine; they use only software code for SSLVPN (even onboard crypto engine enabled).

- CSCsq97517

  Symptoms: On a newly-rebooted router, CEF states on SP will not be in sync with RP.

Conditions: It is a very rare race condition that triggers this problem. It is not seen on many platforms.

Workaround: There is no workaround, other than reloading the router.

- CSCsq98742

  Symptoms: A Cisco AS5400 router crashes frequently with Cisco IOS Release 12.4 (19b) attempting to free memory for X28 component.

  Conditions: This symptom is observed on a Cisco AS5400.

  Workaround: There is no workaround.

- CSCsr05992

  Symptoms: A router crashes when it tries to create a version 9 template field for pfr configurations.

  Conditions: This symptom is observed if pfr subflow is configured for NetFlow version 9 export.

  Workaround: Disable pfr configurations.

- CSCsr10075

  Symptoms: Under very rare timing condition, an OSPF Type-5 route may stay in the routing table after the adjacency is lost over ISDN/virtual-access interface.

  Conditions: The problem is seen only in Cisco IOS versions that do not have integrated CSCeh23420. Cisco IOS versions with CSCeh23420 are not affected.

  Workaround: Clear IP route for the route, which is stuck in the routing table. Upgrade to a Cisco IOS version that are integrated with CSCeh23420 or CSCsr10075.

- CSCsr10484

  Symptoms: Router crashes when the **show policy-map interface** command is entered.

  Conditions: Occurs during the following scenario:

  1. Attach a policy-map that has queuing and non-queuing features on a vtemplate and verify functionality.

  2. Shut the physical interface on which the vaccess is built.

  3. Attach the same policy-map on the physical interface. This will work as after the vaccess goes down, the Q stats are disabled (and the HQF hierarchy deleted).

  4. Bring up the physical interface with a **no shut** command.

  5. Vaccess also comes up; issuing the **show policy-map int** command causes the crash.

  Workaround: There is no workaround.

- CSCsr13521

  Symptoms: Memory chunk allocated for LDP-IGP Sync may leak.

  Conditions: The symptom is observed on a router with a dual link to its neighbor. LDP and LDP Graceful Restart are enabled on both routers. When LDP is disabled and re-enabled globally on the neighbor router, a small memory leak occurs on this router.

  To verify the memory leak, on Router 1, enable memory leak debug with the **set memory debug incremental starting-time** command. On Router 2, disable LDP globally with the **no mpls ip** command. Wait for LDP session go down, then re-enable LDP. On Router 1, the memory chunk leak for LDP should be seen with the **show mem debug leaks chunks** command.

  Workaround: There is no workaround.

- CSCsr17680

  Symptoms: AA-request, sent to a particular server, getting failed-over to all other servers in the server group, when the first server is not responding or first server is unreachable.

  Conditions: This issue is observed when sending request to particular server on a server-group.

  Workaround: There is no workaround.

- CSCsr17719

  Symptoms: A crash may be observed from name_age_cache API.

  Conditions: There is no specific situation under which this crash is seen.

  Workaround: There is no workaround.

- CSCsr18073

  Symptoms: When polling the IP SLA Ethernet MIB, the switch returns an incorrect value for "Destination to Source positive jitter Sum2." Instead, the switch returns the value for "Source to Destination positive jitter Sum2."

  Conditions: The symptom is observed when the IP SLA Ethernet MIB is polled.

  Workaround: There is no workaround.

- CSCsr18691

  Cisco IOS devices that are configured with Cisco IOS Zone-Based Policy Firewall Session Initiation Protocol (SIP) inspection are vulnerable to denial of service (DoS) attacks when processing a specific SIP transit packet. Exploitation of the vulnerability could result in a reload of the affected device.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available within the workarounds section of the posted advisory.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-ios-fw.shtml

- CSCsr20566

  Symptoms: A router may log SCHED-3-STUCKMTMR for Dampening process, after which point all dampened interfaces will be permanently dampened from a routing-protocol viewpoint.

  Conditions: This symptom is observed when multiple interfaces are configured with dampening feature.

  Workaround: There is no workaround.

- CSCsr20889

  Symptoms: The system reloads.

  Conditions: The symptom is observed when a dynamic crypto map is added to the existing GETVPN crypto map with a different sequence.

  Workaround: There is no workaround.

- CSCsr24551

  Symptoms: A Cisco 7200 VXR series router may crash and reload upon applying a policy map.

  Conditions: This symptom is observed when the service policy map is applied on the channelized E3 interface of a Cisco 7200 VXR router and traffic is pumped. The issue is observed only for E3 interface.

Workaround: Remove the service policy map.

- CSCsr24997

  Symptoms: There is an uninitialized variable used in stile_api.c which is triggering a compilation warning.

  Conditions: The symptom is observed when an uninitialized variable is triggering a compilation warning: ../stile/stile_api.c: In function ‘stile_populate_protocol_list_entry’: ../stile/stile_api.c:341: warning: ‘type’ might be uninitialized in this function.

  Workaround: There is no workaround.

- CSCsr25788

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

  Conditions: This symptom is observed when NAT is enabled while the router is configured to pass multicast traffic.

  Workaround: There is no workaround.

- CSCsr27305

  Symptoms: A Cisco 1801 router withdraws power to a Polycom 430 IP phone and the phone power-cycles continuously.

  Conditions: The symptom is observed on a Cisco 1801 router with POE-180x daughter card and external power module with default switchport configuration that powers a Polycom 430 IP phone. CDP is enabled so that phone can detect Voice VLAN. The phone requests 4.5 W of power, but the router is only giving 4 W.

  Workaround: Turn off CDP on switchport.

  Further Problem Description: The same Polycom IP phone works correctly on any DSBU POE switch.

- CSCsr27794

  Symptoms: BGP does not generate updates for certain peers.

  Conditions: BGP peers show a neighbor version of 0 and their update groups as converged. Out queues for BGP peers are not getting flushed if they have connection resets.

  Workaround: There is no workaround other than entering the **clear ip bgp *** command.

- CSCsr29691

  Port Address Translation (PAT) is a form of Network Address Translation (NAT) that allows multiple hosts in a private network to access a public network using a single, public IP address. This is accomplished by rewriting layer 4 information, specifically TCP and UDP source port numbers and checksums, as packets from the private network traverse a network device that is performing PAT. PAT is configured by network administrators and performed by network devices such as firewalls and routers in situations where public IP addresses are limited.

  After the initial multi-vendor DNS advisory was published on July 8th, 2008 it was discovered that in some cases the fixes to DNS implementations to use random source ports when sending DNS queries could be negated when such queries traverse PAT devices. The reason for this is that in these cases the network device performing PAT uses a predictable source port allocation policy, such as incremental allocation, when performing the layer 4 rewrite operation that is necessary for PAT. Under this scenario, the fixes made by DNS vendors can be greatly diminished because, while DNS queries seen on the inside network have random source port numbers, the same queries have potentially predictable source port numbers when they leave the private network, depending on the type of traffic that transits through the device.

Several Cisco products are affected by this issue, and if DNS servers are deployed behind one of these affected products operating in PAT mode then the DNS infrastructure may still be at risk even if source port randomization updates have been applied to the DNS servers.

This bug is for Cisco IOS software, which may an incremental source port allocation policy when performing the source port rewrite operation that is needed for PAT. Refer to the following URL for information on when the PAT implementation in Cisco IOS will use an incremental port allocation policy:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6640/product_data_sheet0900aecd8064c999.html

(Paragraph immediately following the first image)

Note that traditional NAT, i.e. allocating one public IP address for each private IP address, is not affected by this problem because, unlike PAT, NAT only rewrites layer 3 information and does not modify layer 4 header information of packets traversing the NAT device.

For more information about the DNS vulnerability mentioned above, please refer to the multi-vendor advisory at:

http://www.kb.cert.org/vuls/id/800113

Or at the Cisco-specific advisory at:

http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml

- CSCsr29468

  Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

- CSCsr37296

  Symptoms: MPLS packets with experimental bit set are not classified according to output service-policy rules.

  Conditions: Occurs when you define an output policy to classify packets by "mpls experimental" bits on output to Multilink:

  class-map match-any *xclass*

  match mpls experimental topmost *5*

  policy-map *xpolicy*

  class *xclass*

  priority percent *99*

  class class-default

  bandwidth percent *1*

  interface Multilink1 service-policy output *xpolicy*

  Workaround: There is no workaround.

- CSCsr40433

  Symptoms: Traffic engineering (TE) tunnel reoptimization fails and tunnel stuck in “RSVP signaling proceeding.”

Conditions: Occurs when explicit path with loose next hops and one of the next hops is still reachable and that next hops is a dead-end.

Workaround: Use strict next hop addresses.

- CSCsr48677

  Symptoms: There may be memory allocation errors and traceback for the Net Background process when HWIC-1FE/2FE is present in the router.

  Conditions: The symptoms are observed when the line protocol state of FastEthernet interface in HWIC-1FE/2FE is down for more than 48 hours.

  Workaround: Configure the **no keepalive** command on the interface that is down.

- CSCsr48828

  Symptoms: A Cisco router may display the following traceback:

  ```
  %SYS-2-GETBUF
  ```

  Conditions: The symptom occurs when ACLs are configured on the WAN interfaces of the router. When outbound packets fail and are dropped on an outbound ACL, a traceback is generated. If the packets are stopped or the ACLs removed, the tracebacks stop. The problem is seen with the VSA accelerator, but not seen when software crypto is used.

  Workaround: There is no workaround.

- CSCsr54170

  Symptoms: A router may crash when removing policy-map configuration with policy-map still in use (with traffic through).

  Conditions: The symptom is observed if a policy-map is removed from configuration and that policy-map is still referenced by an interface service-policy statement (with traffic through).

  Workaround: Stop traffic before removing policies.

- CSCsr59242

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

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

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

  clear ip eigrp vrf abc *as-number*
  neighbors *interface*

  Wait 30 seconds:

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

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

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

- CSCsr61729

  Symptoms: WIC-2AM-V2 and WIC-1AM-V2 card is recognized but the ping functionality may be broken.

  Conditions: The symptoms are observed with a back-to-back connection of WIC-2AM-V2 and WIC-1AM-V2 modules with a third-party vendor connector.

Workaround: There is no workaround.

Further Problem Description: The problem is due to a prior checkin which made the state of the device dependent on the physical connection of the cable. This code was interfering with the software state machine which internally maintains the state of the machine.

- CSCsr62441

  Symptoms: Router is crashing while configuring "connect <word> voice-port 7/0:0 t1 7/0" and tracebacks can be observed.

  Conditions: The symptoms are observed on a Cisco 5400 platform when configuring “connect <word> voice-port 7/0:0 t1 7/0.”

  Workaround: There is no workaround.

- CSCsr62545

  Symptoms/Conditions: RPM-XF cards 9(active) and 11(standby) are in redundancy. When we reset the active card, we see that secondary card 11 comes up as active but primary card 9, instead of coming up as standby, is continuously rebooting, resulting in many crashinfo files being generated.

  Workaround: There is no workaround.

- CSCsr67177

  Symptoms: A router may experience a corner case crash if an IPv6 OSPF router is removed from the configuration.

  Conditions: The following conditions must be met before router is removed from the configuration to experience the system crash: OSPFv3 router does not run because the router-id is not available (it means that no IP address is available and/or router-id is not configured). SW interface is configured, assigned under inactive OSPFv3 router, and later removed using the **no interface** command.

  Workaround: Ensure that when the IPv6 router is configured it runs properly (if it does not start, there is a warning printed on the console advising what action to take).

- CSCsr67788

  Symptoms: IPv6 traffic is classified as IPv4 traffic.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(20)T.

  Workaround: There is no workaround.

- CSCsr69433

  Symptoms: A router may experienc %SYS-3-CPUHOG: errors and then a watchdog crash in the FR LMI process.

  Conditions: The symptoms are observed when ISDN is configured on the router.

  Workaround: There is no workaround.

- CSCsr72352

  Symptoms: EBGP-6PE learned IPv6 labeled routes are advertised to IBGP-6PE neighbor by setting NH as local IP address.

  Conditions: This symptom is observed on 6PE Inter-AS Option C with RR case.

  Workaround: There is no workaround.

- CSCsr82471

  Symptoms: A dial-peer's preference is changed. This problem is observed in any Cisco IOS version since the ephone-hunt secondary preference is supported. The latest images, such as Cisco IOS Release 12.4(20)T1, 12.4(22)T1, and 12.4(22) YB1, also exhibit this issue.

  Conditions: This symptom is observed when ephone-hunt has secondary preference configured.

  Workaround: Remove secondary preference in ephone-hunt.

- CSCsr82895

  Symptoms: When a router has many PPPoE sessions and the router is configured as an RP-mapping agent, the router crashes following a switchover.

  Conditions: The symptom is observed when the router has 8000 PPPoE sessions and it is configured as an RP-mapping agent. Following a switchover, the issue is seen.

  Workaround: Another router that does not have as many interfaces in the network should be configured as the RP-mapping agent.

- CSCsr83547

  Symptoms: Dialer watch on the Cisco 3845 router makes the backup link of PPP multilink on the PRI port which is connected to BRI 4 port of peer router through ISDN net. If one out of four BRI ports is shut down on the peer router, the dialer watch does not keep the backup link up without resetting the idle timer at the expiration of idle timeout though the primary link remains down, causing the other three ports to be disconnected.

  Conditions: This symptom occurs only when the BRI port which contains B-ch that became link up first is shut down. This symptom does not occur even if the other BRI ports are shut down.

  Workaround: There is no workaround.

- CSCsr93764

  Symptoms: Bus error exceptions due to Application Firewall HTTP inspection.

  Conditions: This issue has been seen in several Cisco 3845 routers running Cisco IOS Release 12.4(15)T5 with IP Inspect configured.

  Workaround: There is no workaround.

- CSCsr96042

  Symptoms: ASR1000 Router crashes.

  Conditions: Occurs if "ip vrf" is deleted from the configuration.

  Workaround: There is no workaround.

- CSCsr96753

  Symptoms: A router may crash when entering the **isdn test call** command.

  Conditions: The symptom is observed when the BRI interface is up.

  Workaround: There is no workaround.

- CSCsr97343

  Symptoms: An MSDP peer may flap randomly.

  Conditions: The symptom is observed when the device is configured with **logging host** *ip-address* ... or **logging host** *ip-address*.

  Workaround: It has been observed that removing the "logging host" configuration helps in preventing the peer-flap:

no logging host *ip-address*
no logging *ip-address*

- 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.

- CSCsu00266

  Symptoms: The following crash is observed after configuring a policy-map.

  ```
  SegV exception, PC 0x2142818 at 10:04:23
  ```

  Conditions: Occurred on a Cisco 7206VXR (NPE-G2) running Cisco IOS Release 12.4(15)T5.

  Workaround: There is no workaround.

- CSCsu03038

  Symptoms: Memory leak occurs.

  Symptoms: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(11)T4. Leak rate is very low, approximately 94k over 18 weeks.

  Workaround: There is no workaround.

- CSCsu06350

  Symptoms: T.38 fax call not terminating audio properly.

  Conditions: RE-INVITE from SIP Fax application changes connection IP address in SDP. PGW sends changed IP address in MDCX to GW. GW responds with 200 acknowledging this change. GW still sends audio to IP address where original call terminated.

  Workaround: There is no workaround.

- CSCsu10229

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

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

  Workaround: There is no workaround.

- CSCsu10606

  Symptoms: A device crashes with the following error message:

  ```
  Breakpoint exception, CPU signal 23, PC =0x606CE1B4
  ```

  Conditions: The symptom is observed during Online Certificate Status Protocol (OCSP) use.

  Workaround: There is no workaround.

- CSCsu11522

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS software that can be exploited remotely to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate the vulnerability apart from disabling SIP, if the Cisco IOS device does not need to run SIP for VoIP services. However, mitigation techniques are available to help limit exposure to the vulnerability.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml.

- CSCsu12040

  Symptoms: BGP neighbors that are configured with as-override and send-label (CsC) together may not work after an interface flap or service reset.

  Conditions:

  neighbor *xxx* **as-override**
  neighbor *xxx* **send-label**

  Workaround: Enter the **clear ip bgp * soft in** command.

  Further Problem Description: Peers (neighbors) with a CsC (IPv4+label) BGP configuration with the as-override option should be separated into different dynamic update groups during the BGP update generation process. After the CSCef70161 fix in Cisco IOS Release 12.0(32)SY4, this is no longer the case; this CSCsu12040 fix enhances the CSCef70161 fix to handle the CsC (IPv4+label) case separately.

- CSCsu18232

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

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

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

- CSCsu20411

  Symptoms: A router may crash while unconfiguring “source template test” in interface configuration mode.

  Conditions: The symptom is observed with a router loaded with Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsu21828

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

  Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

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

- CSCsu24087

  Symptoms: A router hangs for a couple of minutes, then crashes anytime the **clear ip bgp neighbor x.x.x in** command is issued.

  Conditions: This symptom occurs when a router crashes when the **clear ip bgp neighbor x.x.x.x soft in** command is issued when the following commands are configured for that neighbor (without route-map):

  1) **neighbor x.x.x.x soft-reconfiguration inbound**

  2) **neighbor x.x.x.x weight** 3) **neighbor x.x.x.x filter-list in**

  If any one of the commands is not configured, then the router will not crash.

  Workaround: Configure route-map instead of filter-list for inbound direction. For example: "neighbor x.x.x.x filter-list 1 in" replace with "neighbor x.x.x.x route-map *name* in".

  Where, route-map *name* permit 10 match as-path 1.

- CSCsu25797

  Symptoms: When the router is running with an on-board VPN module, the module driver should update the maximum IKE SA limit to support more tunnels than software encryption. However, the on-board driver may not update the limit when Cisco IOS Release 12.4(11)T or later is used. Therefore, only 100 IKE SA are supported with the on-board module.

  Conditions: The symptom is observed with a Cisco 2811 or 2821 router that is running Cisco IOS Release 12.4(11)T or later.

  Workaround: Use Cisco IOS Release 12.4(9)T.

- CSCsu25833

  Symptoms: An ISR router may crash with the following error message:

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

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

  Workaround: There is no workaround.

- CSCsu26174

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

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

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

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

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

- CSCsu26526

  Symptoms: Memory leak can be seen on the LNS.

  Conditions: The symptom is observed on the L2TP Network Server (LNS) when the PPP client does a renegotiation.

  Workaround: There is no workaround.

- CSCsu27888

  Symptoms: IGMP v3 reports are discarded.

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

  Workaround: There is no workaround.

- CSCsu32104

  Symptoms: A PRE-3 that is running Cisco IOS Release 12.2(31)SB code may encounter a Redzone overrun memory corruption crash.

  Conditions: Unknown at this time.

  Workaround: Turn off Auto IP SLA MPLS by entering the **auto ip sla mpls reset** command.

- CSCsu32154

  Symptoms: Calls through an MGCP-controlled FXS may fail to complete. The user will hear fast-busy signal when attempting to make inbound or outbound calls from or to that port. Outbound calls to the port in this state may return a 400 error “Previous message in-progress” in response to the CRCX.

  Conditions: The symptom is observed under rare conditions with an MGCP-controlled FXS port on a Cisco IOS Voice over IP (VoIP) gateway.

  To verify that a port is in this state, compare the output of **show mgcp connection** to the output of **show voice call summary**. If a call appears with the mgcp show command output for a port but that port appears idle (FXLS_ONHOOK) in the voice call output, this would indicate the problem being seen.

  An example of such output is here showing port 2/1 in this state:

  VG224# show voice call summ PORT CODEC VAD VTSP STATE VPM STATE
  ============== ========= === ==================== ====================
  2/0 - - - FXSLS_ONHOOK 2/1 - - - FXSLS_ONHOOK

  VG224# show mgcp conn Endpoint Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent [SIFL] (R)esult[EA (ME)dia (COM)Addr:Port 1. aaln/S2/1 C=,34,-1 I=0x0 P=0,0 M=0 S=9,0 CO=0 E=3,10,10,10 R=41,0 ME=0 COM=0.0.0.0:0

  Workaround: Reload the gateway to recover a port once it is in this state. Attempting to restart the MGCP service on the gateway by removing and adding the **mgcp** command in the configuration has been shown at times to be ineffective once in this state.

  Alternate Workaround: Use of H323/SIP signaling instead of MGCP will prevent ports from getting into this state.

  Further Problem Description: Changes applied through CSCsq97697 have been found to greatly reduce the instances of this issue from occurring. If using H323/SIP instead of MGCP is not an option, it is recommended to use a Cisco IOS Release that contains the changes in CSCsq97697 (for example, Cisco IOS Release 12.4(15)T7).

  The changes applied to CSCsu32154 introduce a new MGCP CLI command which is not enabled by default. If upgrading to obtain a fix for this issue, configure **mgcp disconnect-delay**.

- CSCsu33111

  Symptoms: The **shutdown** command is not working as expected and it reloads the NME-16ES-1G Service Module instead.

  Conditions: When the **service-module gigabitEthernet <x/y> shutdown** command is issued from ISR, the NME-16ES-1G Service Module reloads instead of shutting down.

  Workaround: There is no workaround.

- CSCsu35597

  Symptoms: Renaming a directory gives error message.

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

  Workaround: There is no workaround.

- CSCsu35776

  Symptoms: When running zone-based firewall (ZBF), there is a memory leak in the Chunk Manager.

  Conditions: When viewing the memory information with **show processor memory** command, the Chunk Manager process will grow continuously as long as traffic is running. Eventually all memory will be exhausted.

  Workaround: There is no workaround.

- CSCsu35963

  Symptoms: IPIPGW/CUBE will not respond to a H.245 EmptyCapabilitySet (ECS) (i.e. TerminalCapabilitySet(TCS)=0) message from Cisco Voice Portal (CVP) with a CloseLogicalChannel (CLC) message. This will result in call failure.

  Conditions: The symptom occurs when IPIPGW is deployed in H.323-H.323 mode, running Cisco IOS Release 12.4(20)T and interacting with CVP.

  Workaround: There is no workaround.

- CSCsu36836

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

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

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

- CSCsu39338

  Symptoms: Redistributed routes are not removed even though network is down. Redistribution is done between BGP and OSPF.

  Conditions: Occurs on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsu40497

  Symptoms: IPIPGW/CUBE drops the H.245 OpenLogicalChannel(OLC) received from Cisco Voice Portal (CVP). This results in call failure.

  Conditions: This occurs when IPIPGW/CUBE is deployed in H.323-H.323 mode, running Cisco IOS Release 12.4(20)T and registered to a gatekeeper and talking to a CVP server.

  Workaround: Do not register the IPIPGW/CUBE to a Gatekeeper.

- CSCsu42078

  Symptoms: A router may crash due to bus error caused by an illegal access to a low memory address.

  Conditions: This symptom occurs when a service-policy is applied to an interface.

  Workaround: Remove "ip cef distributed" from the configuration.

- CSCsu44789

  Symptoms: Spurious memory access traceback is seen.

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

Workaround: There is no workaround.

- CSCsu45973

  Symptoms: A router may crash very close in time to when an RFC 4938 compliant PPPoE session is being terminated.

  Conditions: The symptom is observed when the VMI interface is in aggregate mode and an RFC 4938 compliant PPPoE session is terminated.

  Workaround: There is no workaround.

- CSCsu46060

  Symptoms: A router may crash under low memory conditions.

  Conditions: The symptom is observed with a router running GetVPN and Cisco IOS Release 12.4(15)T7.

  Workaround: There is no workaround.

- CSCsu47027

  Symptoms: A device may crash 10-15 times per day when receiving calls from a end customer using a third party-vendor PBX.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(21) and Release 12.4(20)T.

  Workaround: There is no workaround.

- CSCsu47660

  Symptoms: A line flaps.

  Conditions: The problem is observed on an E1 link with HDLC and PPP encapsulation. Cisco Express Forwarding (CEF) is enabled.

  Workaround: Disable CEF.

- CSCsu48898

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

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

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

- CSCsu50873

  Symptoms: The PBR Next Hop Recursive feature does not function unless CEF is disabled on the corresponding interface.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(20)T.

  Workaround: There is no workaround.

- CSCsu51668

  Symptoms:

  1. A router may crash when reattaching a map-class or accessing the time-slots in controller mode.

  2. A router may crash when doing an OIR or flapping the peer interface.

  Conditions: The symptoms are observed on a Cisco 7200 series router that is configured for HQF and FRF.12.

Workaround: There is no workaround.

- CSCsu53032

  Symptoms: In rare cases, a router will crash upon removing a trustpoint in global configuration mode.

  Conditions: This defect will occur in all Cisco IOS platforms; however the symptoms observed may differ. Many platforms will handle this gracefully, while others do not, due to different hardware handling of memory errors. The only platforms that have reported intermittent crashes to date are the Cisco 831, Cisco 871, and Cisco 3845.

  Workaround: Reload the router and use a version with the fix.

- CSCsu54436

  Before you use an AP801 Series Lightweight Access Point with controller software release 5.2, you must upgrade the software in the Cisco 800 Series Integrated Services.

- CSCsu54801

  Symptoms: IPv6/IPv6 tunnel adjacency information is incomplete on the line card. This prevents IPv6/IPv6 multicast traffic on the tunnel.

  Conditions: The symptoms are observed under normal operation.

  Workaround: There is no workaround.

- CSCsu60252

  Symptoms: A Cisco router may unexpectedly reload when running IPS.

  Conditions: The symptom is observed when either the “deny-attacker-inline” or the “deny-connection-inline” event actions are configured on at least some of the IPS signatures. The default event action is always just to alarm, so additional configuration is required to cause this particular crash.

  When the “deny” event actions are configured, the router may crash if a “shun acl” is applied on an interface where IPS is NOT configured.

  This can happen in a situation such as in the following example, if IPS is configured on E0 but not E1:

  E0 (packet triggering the alarm) --> ROUTER <-- (attacker) E1

  IPS is configured on E0 and a packet which triggers an alarm comes in on E0. This packet matches a signature which has the "swap-attacker-victim" parameter in its signature definition. Therefore, if a "deny" event action has been configured, the ACL will be created on E1. If IPS is NOT configured on E1, this scenario can trigger the crash.

  Workaround: If the “deny” actions are being used, a workaround would be to configure IPS on all affected interfaces.

- CSCsu61665

  Symptoms: A router may crash upon session establishment or termination over a VMI interface with "debug vmi pppoe" enabled.

  Conditions: The symptom is observed when "debug vmi pppoe" is enabled and a session is initiated or terminated.

  Workaround: Disable "debug vmi pppoe".

- CSCsu61953

  Symptoms: In 6VPE topology, IPv6 routes are not propagated properly to the 6VPE neighbor. Although the IPv6 prefixes are included in the update message, they are sent in an invalid format. On the receiving router, the decoded IPv6 prefix is a different entry compared to the actual prefix sent. This causes the actual IPv6 prefix to be lost and not propagated further.

  Conditions: The symptom only occurs in 6VPE cases with a non-connected nexthop and when an IPv4-mapped IPv6 nexthop is to be sent. The nexthop field is not set properly.

  Workaround: There is no workaround.

  Further Problem Description: The root cause is discrepancy in the macro values assigned to indicate "no label" in different release trains. In one of the functions, this macro got misplaced in wrong code. When the prefix outtag is compared with the wrong macro value mentioned above, then the gateway of the prefix or the nexthop is not set properly. The nexthop instead of being set to an IPv4-mapped IPv6 address, is set to the global IPv6 nexthop. Since this is not a connected nexthop, the label allocation is not done. This message with 6PE prefix when received on the other end, is decoded as though the label exists. So the prefix retrieved from the message will be different from the actual prefix sent and hence the problem.

- CSCsu62667

  Symptoms: LSP ID change after stateful switchover (SSO) due to failure in signaling recovered label switched path (LSP).

  Conditions: Occurs following a SSO switchover.

  Workaround: There is no workaround.

- CSCsu62921

  Symptoms: %SYS-2-BADSHARE tracebacks are reported. Eventually the router will stop passing all traffic over the interface.

  Conditions: Occurs when sending traffic over xDSL interfaces that have QoS configured.

  Workaround: Remove the service-policy from the xDSL interface.

- CSCsu64215

  Symptoms: Router may incorrectly drop non TCP traffic. TFTP and EIGRP traffic can be impacted as seen in CSCsv89579.

  Conditions: Occurs when the **ip tcp adjust-mss** command is configured on the device.

  Workaround: Disable the **ip tcp adjust-mss** command on all interfaces. Note that this may cause higher CPU due to fragmentation and reassembly in certain tunnel environments where the command is intended to be used.

- CSCsu64323

  Symptoms: The **show vpdn history failure** command should show the history of session failures due to entering incorrect password, but it does not show any history.

  ```
  Router# show vp hi fa

  % VPDN user failure table is empty
  ```

  Conditions: The problem was seen with a Cisco 7201 that is running Cisco IOS Release 12.2(33)SRC1. No problem with Cisco IOS Release 12.4(4)XD9.

  Workaround: There is no workaround.

- CSCsu65189

  Symptoms: If router is configured as follows:

  router ospf 1
  ...
  passive-interface Loopback0

  And later LDP/IGP synchronization is enabled using the following commands:

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

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

  Router# show ip ospf mpls ldp in

  Loopback0
  Process ID 1, Area 0
  LDP is not configured through LDP autoconfig
  LDP-IGP Synchronization : Required < ---- NOK
  Holddown timer is not configured
  Interface is up

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

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

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

  The problem will not occur if LDP/IGP sync is already in place and:

  - -Router is reloaded with image with fix for CSCsk48227.
  - -Passive-interface command is removed/added.

- CSCsu67369

  Symptoms: A router with a VSA may crash if it receives high levels of inbound clear traffic.

  Conditions: The symptom is observed on a Cisco 7200 series router with a VSA that receives high levels of inbound clear traffic which should have been encrypted when it is downloading large number of GETVPN SAs.

  Workaround: There is no workaround.

- CSCsu67461

  Symptoms: Router may crash when "show tracking brief" is entered if one or more tracking object have been created using the Hot Standby Routing Protocol (HSRP) cli, such as **standby 1 track Ethernet1/0**.

  Conditions: This does not occur if all tracking objects use the new **track** command as follows:

  track 1interface Ethernet1/0 line-protocol
  interface Ethernet 0/0
  standby 1 track 1

  Workaround: Use **show tracking** instead, or configure tracking with the new command.

- CSCsu68245

  Symptoms: A router may crash.

  Conditions: The symptoms are observed when traffic is flowing and if the interface is shut then unshut.

  Workaround: There is no workaround.

- CSCsu69750

  Symptoms: MTP is not able to handle G729a codec and G729 codec on both call legs at same time.

  Conditions: The symptoms are observed with Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

  Further Problem Description: If enabling "debug sccp all", the debug output indicates that it is an "Unsupported mtp req".

- CSCsu70214

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsu70909

  Symptoms: If an ICMP connection is initiated from outside to a global address of a static NAT translation and zone-based firewall (ZBF) is configured, matching that flow, the resulting echo reply will be denied.

  Conditions: This issue was observed on a Cisco 3845 running Cisco IOS Release 12.4(20)T. ZBF was configured in both directions and a static NAT was involved. The outside host was pinging the global NAT address.

  Workaround: Creating a class-map that matches protocol ICMP and applying that to both inside-to-outside and outside-to-inside policy-maps with a pass allows the traffic to flow.

  Further Problem Description:

  Inspect Number of Half-open Sessions = 1 Half-open Sessions Session 682674E0 (10.2.2.2:8)=>(10.1.1.205:0) icmp SIS_OPENING Created 00:00:11, Last heard 00:00:00 ECHO request Bytes sent (initiator:responder) [96:0]

  The session is created, but stuck int eh SIS_OPENING status and last heard is the ECHO request. The packet was actually dropped by ZFW. It appears that it did not match the intended class-map and fell to class-default.

  *Sep 22 22:45:17.707: %FW-6-LOG_SUMMARY: 8 packets were dropped from 10.2.2.2:8 => 10.1.1.205:0 (target:class)-(outside-to-inside:class-default)

  Passing in the class-default class-map in the outside-to-inside policy-map does not allow the traffic to flow. Additionally passing in the class-default class-map in the inside-to-outside policy-map does not allow the traffic to flow.

- CSCsu71728

  Symptoms: A crash may occur while applying QOS under an MFR interface.

  Conditions: The symptoms are observed while applying QOS under an MFR interface on a PA-MC-2T3-EC in L2VPN.

  Workaround: There is no workaround.

- CSCsu71853

  Symptoms: Transfer calls are failing due to the fact that the router does not have anything for "Replaces:" and "Referred-By:" fields.

  Conditions: Occurs in routers running Cisco IOS Release 12.4(15)T6 and Cisco IOS Release 12.4(15)T7.

  Workaround: There is no workaround.

- CSCsu73128

  Symptoms: Router crashes.

  Conditions: Occurs when large number of remote end points try to connect to the gateway at the same time. The router may crash if "rsa-sig" is used as authentication method.

  Workaround: There is no workaround.

- CSCsu73970

  Symptoms: Applying a service policy to an outbound interface causes CPUHOG messages of the following nature, and then it triggers a software-forced crash:

  ```
  %SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs (25/1),process
  = IP Input.
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = IP Input.
  %Software-forced reload
  Preparing to dump core... *Sep 23 22:44:39.275 AWST: %SYS-3-CPUYLD: Task ran for
  (128072)msecs, more than (2000)msecs (25/1),process = IP Input
  22:44:42 AWST Tue Sep 23 2008: Breakpoint exception, CPU signal 23, PC = 0x4004FE88
  ```

  Conditions: This symptom is observed when a service policy is applied to an outbound interface. The service policy should have similar ICMP permit statements:

  permit icmp any 172.16.156.16 0.0.0.15 echo-reply permit icmp any 172.16.156.16 0.0.0.15 echo

  The hang occurs when both of these statements are configured at the same time.

  Workaround: There is no workaround.

- CSCsu76540

  Symptoms: An extension number in an ephone hunt group may not be reached.

  Conditions: The symptom is observed if an ephone in a hunt group (longest- idle) is put on hold by an internal caller. The hunt group will stop trying to hunt this ephone.

  Workaround: Re-configure this ephone hunt group.

  Further Problem Description: When all the ephones in the hunt group are put on hold, this hunt group can not be reached, even when all the ephones are onhook.

- CSCsu76993

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

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

  Workaround: There is no workaround.

- CSCsu77945

  Symptoms: Performance Routing (PfR) echo probe shows 0 completes, even when the **debug icmp** command shows that the reply was correctly received.

  Conditions: The symptom is observed when using the **show oer border active-probes** command, which shows the active probes as incomplete even if the reply was correctly received.

Workaround: There is no workaround.

Further Problem Description: IP SLA code invoked by OER sets the completions to zero.

- CSCsu78553

  Symptoms: Spurious memory found in sslvpn_create_session procedure.

  Conditions: The symptom is observed when SSLVPN is configured.

  Workaround: There is no workaround.

- CSCsu84383

  Symptoms: When a policy from MLP virtual access is removed, the router may crash in queuing enqueue.

  Conditions: The symptoms are observed under the following conditions:

  - Vtemplate is configured with multilink PPP.
  - This vtemplate is referred in ATM VC (thus we have PPP over ATM).
  - Attach a queuing policy to vtemplate (that results in inheriting policy on vaccess).
  - Now remove the policy from vtemplate. This results in a crash at HQF enqueue function.

  Workaround: There is no workaround. HQF queuing is not supported on vaccess interfaces.

- CSCsu88745

  Symptoms: SCCP phones fail to register with Cisco Unified CallManager Express (CME).

  Conditions: Occurs when auto register is enabled without ephone/ephone-dn configuration.

  Workaround: Configure ephone and ephone-dn for all SCCP phones.

- CSCsu92395

  Symptoms: Router crashes.

  Conditions: This issue occurred on a Cisco 870 router running Cisco IOS Release 12.4(15)T7 and Release 12.4(20)T with EEM configuration like the following:

  event manager applet RTR-MYPRIVATE_DOWN trap
  event syslog pattern "\%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down"
  action Mail mail server "mailaddress@cisco.com" to "mailaddress@cisco.com" from "mailaddress@cisco.com" subject "rtr-myprivate - down" body "Sorry, I'm Down"
  event manager applet RTR-MYPRIVATE_UP trap
  event syslog pattern "\%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up"
  action Mail mail server "mailaddress@cisco.com" to "mailaddress@cisco.com" from "mailaddress@cisco.com" subject "rtr-myprivate - up" body "Hi, I'm Active now"

  When Virtual-Access1 interface flaps the box crashes.

  Workaround: Remove EEM action mail configuration.

- CSCsu92432

  Symptoms: The router's async line used for reverse SSHv2 might hang after a failed authentication and not recover unless the router is rebooted. The router log displays:

  ```
  %SYS-3-HARIKARI: Process SSH Process top-level routine exited
  ```

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

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

- CSCsu95319

  Symptoms: Igmp-proxy reports for some of the groups are not forwarded to the helper. This causes members not to receive the multicast traffic for those groups.

  Conditions: The problem is seen when the igmp-proxy router is receiving UDP control traffic. That is, the router is receiving any UDP control-plane traffic on any interface.

  Workaround: There is no workaround.

- CSCsu97177

  Symptoms: Device may reload while querying the CISCO-IETF-IP-FORWARD (IPv6) MIB.

  Conditions: SNMP must be configured on the device, and the querier must be aware of the appropriate community to use. Further, there must exist multiple IPv6 global routing tables on the device. This will only be the case if VRFs have been configured with the "vrf definition" command, and that vrf has the IPv6 address family configured, and if that VRF is applied to an interface and global IPv6 addresses configured. This can be confirmed by the existence of multiple tables marked "global" in the output of the "show ipv6 table" command.

  Workaround: Exclude the CISCO-IETF-IP-FORWARD from queries.

  Further Problem Description: Ensure that SNMP is configured so that it can only be accessed by authorized users.

- CSCsu97507

  Symptoms: After removing one of "ip name-server xxxx" entries, the **show ip dns view** command displays broken output.

  Conditions: The symptoms are observed with the following steps:

  1. Add several "ip name-server xxxx".

  2. Remove one of the middle entries.

  3. Use the **show ip dns view** command.

  Workaround: There is no workaround.

  Further Problem Description: This issue has been recreated with Cisco IOS Releases 12.4(15)T5, 12.4(15)T7, and 12.4(20)T.

- CSCsu97934

  Symptoms: NPE-G1 is crashing with "pppoe_sss_holdq_enqueue" as one of the last functions.

  Conditions: Unknown.

  Workaround: Enter the **deb pppoe error** command to stop the crashing.

- CSCsu98241

  Symptoms: Unconfiguration and reconfiguration is putting the MR in a down state.

  Conditions: This symptom is observed when the whole MR configuration is removed and added.

  Workaround: Reload to bring the MR to a run state.

- CSCsv00168

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

  Conditions: The symptoms are observed with Cisco IOS Release 12.4(23.2)T.

  Workaround: There is no workaround.

Further Problem Description: The CLI function is not affected by the junk values.

- CSCsv00959

  Symptoms: A crash occurs.

  Conditions: This symptom is observed after IPv6 unicast routing is unconfigured and only when EIGRPv6 is configured.

  Workaround: There is no workaround.

- CSCsv01474

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

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

  1. The interface flaps.

  2. The **clear ip route** command is issued.

  3. The **no network <prefix>** command and then the **network <prefix>** command are issued for the network corresponding to the interface.

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

- CSCsv04275

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

  ```
  <date>: %ATM_AIM-5-CELL_ALARM_UP: Interface ATM<if ID> lost cell delineation. <date>:
  %ATM_AIM-5-CELL_ALARM_DOWN: Interface ATM<if ID> regained cell delineation.
  ```
  The link may go down and then recover automatically.

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

  Workaround: There is no workaround.

- CSCsv04674

  Symptoms: The M(andatory)-Bit is not set in Random Vector AVP, which is a must according to RFC 2661.

  Conditions: This symptom is observed with Egress ICCN packet with Random Vector AVP during session establishment.

  Workaround: There is no workaround.

- CSCsv04733

  Symptoms: A LAC might terminate a tunnel unexpectedly.

  Conditions: This symptom is seen when the tunnel password exceeds 31 characters.

  Workaround: Use a shorter password if policy allows.

  Further Problem Description: This is seen with Cisco IOS interim Release 12.2 (34.1.3)SB1. With a customer specific special based on Cisco IOS Release 12.2 (31)SB11, it allowed 64 characters.

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In

some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

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

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

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

- CSCsv06608

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

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

  Workaround: There is no workaround.

- CSCsv11142

  Symptoms: A call is disconnected during call resume in a sip-h323 call.

  Conditions: This symptom is observed under the following conditions:

  1) Call was held with ReInvite->ECS.

  2) Received call resume ReInvite.

  3) Capabilities exchanged on H323 leg.

  4) Sent OLC.

  5) Upon receiving OLCAck, CUBE should send ReInvite on the SIP leg; instead it sends 200OK.

  Workaround: There is no workaround.

- CSCsv12795

  Symptoms: Control Plane Policing (CoPP) is not matching or policing ICMP packets correctly.

  Conditions: This symptom is observed with routers that are configured with DMVPN and that are running Cisco IOS Release 12.4(15.3)T (or a later release).

  Workaround: There is no workaround.

- CSCsv13562

  Symptoms: A router crashes because of double free scenarios. While handling a 302 response, "ccb->call_info.origRedirectNumber" attempts a double free because of signaling forking. The following message appears in the crashinfo file:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (2/1),process =
  CCSIP_SPI_CONTROL.
  ```

  Conditions: This symptom is observed when Call Manager Express is running.

  Workaround: There is no workaround.

- CSCsv13738

  Symptoms: There are two ways to define VRFs when supporting the 6VPE feature: 1) ip vrf 2) vrf definition. The "vrf definition" configuration may take a much longer time to allow convergence between the PE and the CE than the "ip vrf" configuration.

Conditions: The symptoms are observed under the following conditions:

- When the router boots up; and
- When the issue has been seen using the "vrf definition" configuration; and
- When the router has over 100,000 VPNv4 BGP routes; and
- When a large number of VRFs are configured.

Workaround: Use the "ip vrf" configuration, if you have only IPv4 VRFs configured.

- CSCsv14530

  Symptoms: This issue happens when anyconnect vpn client is used in standalone mode to connect to the vpn gateway. Whenever a new session with this vpn client is established, it requests a set of files that are served by the gateway. While serving these files, a leak happens.

  Conditions: This leak has been observed on a Cisco 2811 that is running Cisco IOS Release 12.4(20)T and whenever a standalone anyconnect client is used to establish the session.

  Workaround: Use anyconnect web install.

- CSCsv14826

  Symptoms: An EasyVPN tunnel may get stuck in an IPSEC_Active state after a dialer interface flap. The ISAKMP SA can get stuck in Config_XAuth state after the dialer interface flaps:

  ```
  Router: show crypto isakmp sa

  IPv4 Crypto ISAKMP SA
  dst src state conn-id slot status
  10.10.10.10 10.10.10.11 CONF_XAUTH 2090 0 ACTIVE
  ```

  Conditions: The symptoms are observed when EasyVPN is configured on a router and where a dialer interface flaps often.

  Workaround: There is no workaround.

- CSCsv15266

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

  ```
  %SYS-2-FREEFREE: Attempted to free unassigned memory at XXXXXXXX, alloc XXXXXXXX,
  dealloc XXXXXXXX
  ```
  OR
  ```
  %SYS-6-BLKINFO: Corrupted magic value in in-use block blk XXXXXXXX, words XX, alloc
  XXXXXXXX, Free, dealloc XXXXXXXX, rfcnt X
  ```
  Conditions: The reset is triggered by a configuration change tied to QoS and has been seen while changing one of the following:

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

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

- CSCsv17370

  Symptoms: Some applications do not work properly when VSA is used as the crypto engine in the hub router. In the trace, you might observe TCP checksum corruption. This is not true in all cases. However, it might be a symptom if in the sniffer trace taken on the application client server, the last packet received before terminating the application is around 56 to 64 bytes.

  Conditions: This symptom might happen in a very specific scenario. As a condition, you need to have a VSA on the hub router, and the client and server application needs to be in two different remote locations connected via a VPN tunnel through the hub. In addition, the issue has been verified with a tunnel that is configured with a static crypto map. This issue has also been verified with Fast Ethernet ports only.

  Workaround: Disable the crypto engine or use VAM2+.

- CSCsv20058

  Symptoms: Upon digit_end on the RFC-2833 side, the IPIP GW misinterprets this and sends out h245-alphanumeric, which is duplicate. Typically, the IPIP GW should ignore all the tone packets after the digit_begin is detected until the digit_end.

  Conditions: RTP-NTE to H245-Alphanumeric conversion is triggering this event.

  Workaround: There is no workaround.

- CSCsv21930

  Symptoms: The Embedded Event Manager is not available in the Cisco 860 platforms.

  Conditions: Customers that are running the Cisco 860 platform will not be able to use the Embedded Event manager, which includes the "event manager ..." configuration commands.

  Workaround: There is no workaround.

- CSCsv23797

  Symptoms: A Cisco ASR router goes down.

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

  Workaround: Use regular SCP.

- CSCsv24742

  Symptoms: A Cisco router may report exit link out of policy (OOP) when the 32-bit interface utilization counter wraps. At 100-Mbps traffic rate, this can happen once every 6 minutes.

  Conditions: The symptom is observed on a Cisco router running Performance Routing (PfR) and when the 32-bit interface utilization counter wraps.

  Workaround: There is no workaround.

- CSCsv28806

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

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

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

- CSCsv30075

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

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

Workaround: There is no workaround.

- CSCsv38166

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

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

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

  Cisco has released free software updates that address this vulnerability.

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

  This advisory is posted at the following link:

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

- CSCsv40178

  Symptoms: DMVPN setup, where originally the hub and all the spokes were running Cisco IOS Release 12.4(15)T. CDP is enabled on the tunnel interfaces, and the hub was able to see all the spokes as "CDP neighbor." The customer upgraded a few spokes to Cisco IOS Release 12.4(20)T, after which these spokes were no longer seen as CDP neighbors. The other spokes that were running Cisco IOS Release 12.4(15)T were still seen as CDP neighbors.

  Conditions: This symptom is observed under the following conditions:

  - DMVPN network tunnels configured as mGRE.
  - CDP enabled in the tunnel interface.
  - Running new Cisco IOS Release 12.4(2x)Tx image.
  - Crypto enabled or disabled in the tunnel interface.

  Workaround: Downgrade to Cisco IOS Release 12.4(15)Tx. It is not affected.

  It works fine if running a new Cisco IOS Release 12.4(2x)Tx image and using point-to-point GRE in the tunnel interface.

- CSCsv40404

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

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

  Workaround: There is no workaround.

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

- CSCsv40924

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

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

  Workaround:

  1) Configure the **no-payload** command for the NAT translation. This will stop the corruption, but will also cause all deep packet NATing to stop, which can cause other issues.

  2) Use a port other than 554 for the RTSP steam. This will stop the corruption, but will also stop the router from NATing the embedded IP addresses in the RTSP packets. Depending on the specific implementation of RTSP, this may or may not stop the stream from working.

  3) Change your NAT translation such that the private and public IP addresses have the same number of characters. For instance 192.168.0.1 has 11 characters, and 172.16.100.200 has 14 characters.

- CSCsv42721

  Symptoms: UUT that is configured as AP with EAP-FAST configurations fails to associate with the PC client (with appropriate profiles in place). The "show dot11 assoc" command output shows that state is stuck at "AAA_Auth".

  Conditions: Association fails between with UUT/AP and PC client with EAP-TLS configurations.

  Workaround: There is no workaround.

- CSCsv43385

  Symptoms: Connectivity from a DMVPN hub router to spokes may be lost due to a invalid CEF adjacency.

  If tunnel protection is configured on the HUB, the traffic from hub to spokes will get dropped on the tunnel interface and the show interface tunnelx command will show the “Total output drops” counter incrementing.

  This is intermittent and the problem will generally appear right after a reload of the router. It may not happen after some reloads of the router.

  Conditions:

  1) Seen only in Cisco IOS Release 12.4(20)T and 12.4(22)T.

  2) Reload of the router.

  Workaround 1:

  Disable/enable the tunnel mode:

```
interface Tunnel30
 no tunnel mode gre multipoint
 tunnel mode gre multipoint
```

  Workaround 2:

  Remove the tunnel configuration and re-add it:

```
no interface Tunnel30
interface Tunnel30
 ip address 192.168.50.1 255.255.255.0
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 111
```

```
ip nhrp holdtime 900
tunnel source FastEthernet0/0
tunnel mode gre multipoint
```

- CSCsv43444

  Symptoms: A router will run out of memory when SIP phones register.

  Conditions: Cisco 3911 phones are installed.

  Workaround: Disable MWI.

- CSCsv43658

  Symptoms/Conditions: Given a service policy that is already in use by the PDPs of an APN, if the same service policy is applied to another APN, the GGSN crashes.

  Workaround: This crash will not happen if unique service policies are applied to each APN. For example, if service policy ggsn1 is applied to apn1.com, then service policy ggsn2 should be applied to apn2.

- CSCsv45669

  In a PPPoATM setup with the usage of cloned virtual-access subinterfaces and an EIGRP neighbor established over that PPPoATM connection.

  When the ATM interface carrying the PVC in use for the PPPoATM session is shut down. And then subsequently reenabled again, after the EIGRP neighbor and PPPoATM session have timed out.

  We see a problem to reestablish the EIGRP neighborship. The symptom is that the all EIGRP router multicast address, 224.0.0.10, is not bound to the cloned virtual-access subinterface. And as such, the EIGRP process does not see the hello packets from its neighbors and is not forming an EIGRP neighbor.

  Workaround: Configure the following in global configuration mode:

  ```
  no virtual-template subinterface
  ```
  This command instructs the router to not clone virtual-access subinterfaces but only main interfaces. With virtual-access main interfaces, we do not see the problem.

- CSCsv46240

  Symptoms: A flow exporter that is configured for v9 may export corrupt data.

  Conditions: This symptom occurs under the following configuration sequence:

  - Create a flow exporter, but do not set any values within the exporter.
  - Create a flow monitor, and apply the exporter to it.
  - Apply the flow monitor to an interface.
  - Configure the destination of the exporter.

  Workaround: Configure the destination of the exporter before applying it to any flow monitors. Alternatively, remove the flow monitor from all interfaces and reapply it, which causes correct export packets to be sent.

- CSCsv48296

  Symptoms: The router reloads with the following:

  ```
  SYS-6-BLKINFO: Corrupted redzone blk
  ```
  Conditions: The configuration **cns image** is active, and a CNS image operation is in progress.

  Workaround: There is no workaround.

- CSCsv50666

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

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

  Workaround: There is no workaround.

- CSCsv50958

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

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

  Workaround: No workaround is known.

- CSCsv51021

  Symptoms: A router reloads.

  Conditions: The router reloads while trying to do a ping between endpoints through MGRE+IPSEC tunnel.

  Workaround: There is no workaround.

- CSCsv52459

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

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

  Workaround: There is no workaround.

- CSCsv54130

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

  Conditions: Initial configuration in Sync mode:

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

  Changing to Async mode:

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

  Workaround: Toggling the encapsulation to PPP sometimes fixes the problem.

- CSCsv58300

  Symptoms: Classification is not done correctly; it is matching the IPsec header instead of matching parameters in the original header despite **qos pre-classify** configuration.

  Conditions: It has been observed in a DMVPN spoke, GRE tunnel with IPsec protection configured with **qos pre-classify** and applying service policy to the physical interface.

Workaround: Classify traffic in ingress service policy marking the traffic. Classify traffic in the egress with the mark inserted in ingress policy.

- CSCsv59334

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

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

  router eigrp 1
  network 10.0.0.0
  network 0.0.0.0

  Rt130# show ip eigrp topo

  EIGRP-IPv4 Topology Table for AS(1)/ID(13.1.1.1)

  Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - reply Status, s - sia Status

  P 13.1.1.1/32, 1 successors, FD is 128256 via Connected, Loopback1 P 20.1.1.0/24, 1 successors, FD is 281600 via Connected, Ethernet1/0 P 10.147.204.64/26, 1 successors, FD is 281600 via Connected, Ethernet0/2 P 10.147.204.0/26, 1 successors, FD is 281600 via Connected, Ethernet0/0

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

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

- CSCsv60775

  Symptoms: EoMPLSoGRE tunnel on a Cisco 1805 fails to forward packets after the tunnel is established.

  Conditions: Approximately the first 200 packets are forwarded, but then the router stops forwarding packets across the tunnel.

  Workaround: There is no workaround.

- CSCsv62225

  Symptoms: A router crashes when PPPoE sessions are cleared and a policy is removed.

  Conditions: This symptom occurs while removing the policy using the **no policy-map** *name* command.

  Workaround: There is no workaround.

- CSCsv63799

  Symptoms: A router may reload if PfR is enabled and the number of flows exceeds the size of the NetFlow cache. This is a stress condition.

  Conditions: This symptom is observed when PfR is enabled (which also enables NetFlow).

  Workaround: A possible workaround is to configure the following:

  ```
  ip flow-cache timeout active 1
  ```

- CSCsv73509

  Symptoms: With “no aaa new-model” authentication happens through local even TACACS is configured. This happens for the EXEC users under vty configuration.

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

  Workaround: There is no workaround.

- CSCsv74695

  Symptoms: Saved aux port configurations are lost after a reload on the Cisco 880 series.

  Conditions: Issue can be recreated by changing the aux port configurations under “line aux 0” when the combo console/aux port on the Cisco 880 series is in the aux port mode, saving the configs to NVRAM, and then reloading the router.

  Workaround: The following configuration changes can be used to work around the issue:

```
line aux 0
 modem InOut
 modem autoconfigure discovery
```

- CSCsv75948

  Cisco IOS Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available and are documented in the workarounds section of the posted advisory.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-ntp.shtml

- CSCsv76110

  Symptoms: Attaching service policy of self-zone policy-map failure to the zone-pair.

  Conditions: When L7 policy-map of service policy-map attached to the L4 policy-map.

  Workaround: There is no workaround.

- CSCsv77046

  Symptoms: DMVPN spoke-to-spoke communication is working through hub if hub router has following command configured:

```
no ip nhrp cache non-authoritative
```

  Conditions: In Cisco IOS Release 12.4(22)T, spoke-to-spoke communication is going through hub if we have nhrp cache non-authoritative disabled in hub. However, if we downgrade to Cisco IOS Release 12.4(15)XY3, it worked just fine even if “ip nhrp cache non-authoritative” is disabled in hub.

  Workaround: Enable “ip nhrp cache non-authoritative” in hub.

- CSCsv79343

  Symptoms: Tracebacks with the following message will be seen after decrypting TCP packet:

```
%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
```

  Conditions: The configs use IPsec over GRE. Crypto map is applied on the tunnel interface, and the packet is first encrypted with IPsec and then encapsulated with GRE. Tracebacks happens after the decryption.

Workaround: Use GRE over IPsec. Apply crypto map on the physical interface to protect GRE traffic. Or use tunnel protection.

- CSCsv86107

  Symptoms: A Cisco 2800 router crashes due to signal 10.

  Conditions: The crash happens while calls are being transferred.

  Workaround: There is no workaround.

- CSCsv86288

  Symptoms: Sending a NETCONF hello reply that contains a “session-id” element will trigger an instant crash. The device will report a reload due to a bus error.

  Conditions: This occurs when sending a hello reply that contains a session-id element. A hello without this element (that is, one that contains only NETCONF capabilities) does not cause a crash.

  Workaround: Send a NETCONF hello without a session-id element.

- CSCsv87146

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

  Conditions: A dynamic translation mapping is removed while traffic is running.

  Workaround: Stop traffic when removing dynamic NAT translation.

  Further Problem Description: NAT translation is created while dynamic mapping is being removed. These entries contain pointers to memory that is no longer available. When these entries are freed, the router crashes due to illegal memory access.

- CSCsv92292

  Symptoms: The following error message is observed when RITE is applied to the interface:

  ```
  011419: Nov 19 17:53:15.422 CST: %SYS-2-BADBUFFER: Attempt to use contiguous buffer as
  scattered src, ptr= 83C60298, pool= 83C6010C -Process= "<interrupt level>", ipl= 4,
  -Traceback= 0x808DF468 0x80059428 0x8139A9C0 0x8139AEA4 0x80374540 0x8079DD5C
  0x803DEB54 0x8040E938 0x8041235C 0x803FAFB0 0x804D0BA8 0x800AEF4C 0x8001A964
  0x8001A964 0x800AF008 0x800B6D80
  ```

  Conditions: The error is observed on a Cisco 181x device with c181x-advipservicesk9-mz.124-15.T6 when RITE is configured on the interface.

  Workaround: Remove the RITE from the interface configuration.

- CSCsv94099

  Symptoms: Traceback may be seen in relay.

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

  Workaround: There is no workaround.

- CSCsv94905

  Symptoms: c2800: crash at xpfGetACLPATNodeFromMessage

  Conditions: Normal Cisco IOS operation.

  Workaround: There is no workaround.

- CSCsw15188

  Symptoms: A router crashes when “debug isdn q931” is enabled.

Conditions: The problem happens when logging debugs from “debug isdn q931” to an external syslog server.

Workaround: Disable the syslog server when doing the debugs.

- CSCsw18988

  Symptoms: A router crashes while configuring the ACL list for webvpn context under config-webvpn-acl mode with Nulls string URL.

  Conditions: The router is loaded with c7200-adventerprisek9-mz.124-23.8.T.

  Workaround: Configure non-empty URL string for ACL list elements.

- CSCsw19335

  Symptoms: A router crashes at sslvpn_lock_vw_ctx when users try to simultaneously access the webvpn context at same time.

  Conditions: The router is loaded with c7200-adventerprisek9-mz.124-23.8.T.

  Workaround: There is no workaround.

- CSCsw22906

  Code is missing when committing CSCsr37296.

- CSCsw23397

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

  Conditions: This seems to be triggered by outbound calls.

  Workaround: There is no workaround.

- CSCsw23664

  RRI is not working as expected with VRF aware IPsec. Routes are created but may not be removed, leaving them stranded in the routing tables. There is no workaround to clear these routes outside of a reload.

  Impacted versions: 12.4(15)T and above.

  This issue is resolved in:

  - 12.4(22)T1
  - 12.4(20)T2
  - 12.4(15)T9

  And 12.4T version as listed in integrated in field in this defect.

- CSCsw30213

  Symptoms: A router crashes on configuring MGCP.

  Conditions: Configure MGCP with CCM configs in gateway This issue is seen if the router is configured with “ccm-manager redundant-host.”

  Workaround: There is no workaround.

- CSCsw31019

  Symptoms: A Cisco router crashes.

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

  Workaround: There is no workaround.

- CSCsw35638

  Symptoms: When a Cisco router is the Merge Point (MP) for a protected TE tunnel, and FRR is triggered, two things happen:

  - The primary LSP goes down, and traffic is lost on the protected tunnel.
  - Any PLR that is downstream of the failure will lose its backup.

  Conditions: When a competitor's router is a point of local repair (PLR) and a Cisco router is a merge point, then when FRR is triggered, the Cisco router drops the backup tunnel (in some cases immediately and in other cases after 3 minutes). This causes the primary tunnel that is protected by this backup to go down. The issue has been identified as related to the fact that session attribute flags (link/node protection desired) are being cleared by the competitor PLR when the Path is sent over the backup tunnel.

  Workaround: There is no workaround.

- CSCsw36750

  Symptoms: Call will be disconnected with 2 ipipgw's.

  Conditions: In SS-DO case when initial renegotiation Re-INVITE received with only change in media direction then CUBE will not send OLC ACK.

  Workaround: There is no workaround.

- CSCsw39039

  Fax server====H323===CCM-----MGCP===GW---ISDN

  MGCP is configured for CA control T38.

  Faxes fail because the DSPs do not up-speed to T38. Hence the gateway never sends a O: *fxr/t38(start) * and the call disconnects.

  Workaround: Downgrade to Cisco IOS Release 12.4(15)T7.

- CSCsw43948

  Symptoms: A Cisco 3845 that is running c3845-spservicesk9-mz.124-13b.bin starts bouncing the frames (which are not destined for itself) on the same interface it has received on when bridging is enabled on one of the interfaces.

  Conditions: The problem happens if bridging is configured on an Ethernet subinterface in the following way:

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

Workaround: If the command “bridge-group 1” is removed from the subinterface, it will not bounce the frames and drop them as expected.

- CSCsw44230

  Symptoms: High CPU is observed with SIP call through NAT. NAT entry timeout timer causes slow entry deletion.

  Conditions: When high volume of SIP calls go through the NAT box.

  Workaround: Fine-tune UDP timeout value.

- CSCsw44760

  Symptoms: icmp-jitter timeout value is lost upon system reload.

  Conditions: The issue occurs upon reload if the timeout is less than the default threshold value of 5000 or the threshold value is not equal to zero.

  Workaround: Set the threshold equal to zero or increase the timeout to greater than or equal to 5000.

- CSCsw47076

  A vulnerability exists in Cisco IOS software where an unauthenticated attacker could bypass access control policies when the Object Groups for Access Control Lists (ACLs) feature is used. Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability other than disabling the Object Groups for ACLs feature. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-acl.shtml.

- CSCsw49170

  Symptoms: VG20X with SCCP controlled FXS ports has switchover to CME-SRST and then switchback to CUCM, and then one-way audio in calls is experienced.

  Conditions:

  – VG20X running Cisco IOS Release 12.4(22)T
  – CME-SRST running Cisco IOS Release 12.4(15)T7
  – CallManger running 7.0

  The VG20X global configuration has the UCM set for version 7.0, as follows:

  ```
  sccp ccm <call-manager-ip-address> id <identifier> version 7.0
  ```

  The VG20X global configuration has the CME-SRST set for version 4.1, as follows:

  ```
  sccp ccm <cme-srst-ip-address> id <identifier> version 4.1
  ```

  Workaround: Enter the following commands:

  ```
  no sccp
  sccp
  ```

- CSCsw50918

  Symptoms: A router crashes at sslvpn_lock_vw_ctx when users try to simultaneously access the webvpn context at same time.

  Conditions: The router is loaded with c7200-adventerprisek9-mz.124-23.11.T.

  Workaround: There is no workaround.

- CSCsw63356

  Symptoms:

  ```
  %SERVICE_MODULE-4-WICNOTREADY: with traceback.
  ```

  and/or

  ```
  WARNING - timeslots command not accepted by service-module % Service module
  configuration command failed: LOCK OBTAIN TIMEOUT.
  ```

Message being seeing when bringing up a WIC-1DSU-T1-V2.

Conditions: In both a Cisco 3825 and a Cisco 3845 where the WIC-1DSU-T1-V2 in WIC slot 3 is not working upon reload / power cycle when they have five WIC-1DSU-T1-V2 (three in WIC slots, two in NM-2W) configured on the router.

Workaround: Possible workarounds are:

- Do a service module reset on the card after the reload.
- Use only four WIC-1DSU-T1-V2 on the routers.
- Downgrade to before Cisco IOS Release 12.4(15)T7.

- CSCsw64933

  Symptoms: A VXML gateway may stop providing audio prompts to caller.

  Conditions: When TTS text contains “&” which is escaped as “&”, the XML parser converts it to “&”. VXML interpreter did not escape it when sending the TTS to server. This causes TTS to generate a parse error.

  Workaround: Remove the “&” in the VXML script.

- CSCsw65138

  Symptoms: CME router will reboot due to process bus error randomly. For image: Cisco IOS Software, 3800 Software (C3825-SPSERVICESK9-M), Version 12.4(20)T1, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Wed 24-Sep-08 18:40 by prod_rel_team

  Conditions: No particular condition but from the stack trace info we can see some sort of ringing event.

  stack trace from initial traceback

  General information:

  Reason: Traceback Platform: Cisco IOS Software, 3800 Version: 12.4(20)T1 Compiled: 24-Sep-08

  Trace:

  Cisco IOS Software, 3800 Software (C3825-SPSERVICESK9-M), Version 12.4(20)T1, RELEASE SOFTWARE (fc3) Technical Support: http:www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Wed 24-Sep-08 18:40 by prod_rel_team Traceback= 0x633E934C 0x62E266B8 0x62E29614 0x620A061C 0x620D51E0 0x620A1394 0x620AC074 0x6206D3AC 0x6206C86C 0x62077774 0x62077934 0x6208B46C 0x62D292E0 0x62D292C4

  Functions:

  0x633E934C : memcpy (+0xec) 0x62E266B8 : cmm_crs_proc_tr_call_ring (+0x364) 0x62E29614 : cmm_notify_trigger (+0x780) 0x620A061C : OB_Setting_Alert (+0xac) 0x620D51E0 : AFW_FSM_Drive (+0x308) 0x620A1394 : OB_FSM_Drive (+0xac) 0x620AC074 : AFW_M_Destination_Action (+0x164) 0x6206D3AC : AFW_Module_Action (+0xe4) 0x6206C86C : AFW_Object_WalkListeners (+0x274) 0x62077774 : AFW_Process_GetCcqEvent (+0x298) 0x62077934 : AFW_Process_GetEvent (+0x160) 0x6208B46C : AFW_Service_Process_Space (+0x128) 0x62D292E0 : r4k_process_dispatch (+0x1c) 0x62D292C4 : r4k_process_dispatch (+0x0)

  Diagnostic:

  Software failure. The bugs listed below, if any, are likely to be the root cause of the problem, and upgrading to a version in which the bug is integrated will most probably solve the issue. Most likely bugs (of a total of 9 matches): - CSCsi22430 - B-ACD Crashes CME 4.2, R Fixed in versions : 12.4(11)XW - CSCsj98457 - CMM: Add traceability, R Fixed in versions : 12.4(11)XW4 -

CSCsj29857 - Transfer to ICD failed after conference AA, R Fixed in versions : 12.4(11)XW2 - CSCsj49982 - CMM: After connected to AA, xfer to sccp and failed to xfer to ICD, R Fixed in versions : 12.4(11)XW3 - CSCsk89685 - call from SIP trunk to route point failed to transfer to agent or dn, R Fixed in versions : 12.4(19.8)PI8 12.4(15)XZ 12.4(22.3)PI10b 12.4(21.14.9)PIC1 - CSCsq85500 - Add CSTA SingleStepTransfer support, R Fixed in versions : - CSCsg77464 - CMM: minor code cleanup, R Fixed in versions : - CSCse59608 - $$CRS:Incorrect processing INVITE w Replace, R Fixed in versions : - CSCsf11430 - CMM: dangling GCID when PRI-UCCX-SCCP-CTCA-PRI, V Fixed in versions :

Google DDTS link:

Perform unfiltered manual queries: Continue from here.

Rsym output:

-Traceback= 0x633E934C[memcpy+0xec] 0x62E266B8[cmm_crs_proc_tr_call_ring+0x364] 0x62E29614[cmm_notify_trigger+0x780] 0x620A061C[OB_Setting_Alert+0xac] 0x620D51E0[AFW_FSM_Drive+0x308] 0x620A1394[OB_FSM_Drive+0xac] 0x620AC074[AFW_M_Destination_Action+0x164] 0x6206D3AC[AFW_Module_Action+0xe4] 0x6206C86C[AFW_Object_WalkListeners+0x274] 0x62077774[AFW_Process_GetCcqEvent+0x298] 0x62077934[AFW_Process_GetEvent+0x160] 0x6208B46C[AFW_Service_Process_Space+0x128] 0x62D292E0[r4k_process_dispatch+0x1c] 0x62D292C4[r4k_process_dispatch+0x0]

stack trace from main router crash

General information:

Reason: not found Platform: Cisco IOS Software, 3800 Version: 12.4(20)T1 Compiled: 24-Sep-08

Trace:

Cisco IOS Software, 3800 Software (C3825-SPSERVICESK9-M), Version 12.4(20)T1, RELEASE SOFTWARE (fc3) Technical Support: http:www.cisco.com/techsupport Copyright (c) 1986-2008 by Cisco Systems, Inc. Compiled Wed 24-Sep-08 18:40 by prod_rel_team Stack trace from system failure: FP: 0x66749230, RA: 0x633E934C FP: 0x66749230, RA: 0x62E266B8 FP: 0x66749270, RA: 0x62E29614 FP: 0x66749320, RA: 0x620A061C FP: 0x66749768, RA: 0x620D51E0 FP: 0x667497A8, RA: 0x620A1394 FP: 0x667497D0, RA: 0x620AC074 FP: 0x66749800, RA: 0x6206D3AC

Functions:

0x633E934C : memcpy (+0xec) 0x62E266B8 : cmm_crs_proc_tr_call_ring (+0x364) 0x62E29614 : cmm_notify_trigger (+0x780) 0x620A061C : OB_Setting_Alert (+0xac) 0x620D51E0 : AFW_FSM_Drive (+0x308) 0x620A1394 : OB_FSM_Drive (+0xac) 0x620AC074 : AFW_M_Destination_Action (+0x164) 0x6206D3AC : AFW_Module_Action (+0xe4)

Diagnostic:

Software failure. The bugs listed below, if any, are likely to be the root cause of the problem, and upgrading to a version in which the bug is integrated will most probably solve the issue. For more background information about router crashes, please check : Router Crashes Troubleshooting

Most likely bugs (of a total of 9 matches): - CSCsi22430 - B-ACD Crashes CME 4.2, R Fixed in versions : 12.4(11)XW - CSCsj98457 - CMM: Add traceability, R Fixed in versions : 12.4(11)XW4 - CSCsj29857 - Transfer to ICD failed after conference AA, R Fixed in versions : 12.4(11)XW2 - CSCsj49982 - CMM: After connected to AA, xfer to sccp and failed to xfer to ICD, R Fixed in versions : 12.4(11)XW3 - CSCsk89685 - call from SIP trunk to route point failed to transfer to agent or dn, R Fixed in versions : 12.4(19.8)PI8 12.4(15)XZ 12.4(22.3)PI10b 12.4(21.14.9)PIC1 - CSCsq85500 - Add CSTA SingleStepTransfer support, R Fixed in versions : - CSCsg77464 - CMM:

minor code cleanup, R Fixed in versions : - CSCse59608 - $$CRS:Incorrect processing INVITE w Replace, R Fixed in versions : - CSCsf11430 - CMM: dangling GCID when PRI-UCCX-SCCP-CTCA-PRI, V Fixed in versions :

Google DDTS link:

Perform unfiltered manual queries: Continue from here.

Rsym output:

FP: 0x66749230[etext(0x634036b4)+0x3345b7c], RA: 0x633E934C[memcpy(0x633e9260)+0xec] FP: 0x66749230[etext(0x634036b4)+0x3345b7c], RA: 0x62E266B8[cmm_crs_proc_tr_call_ring(0x62e26354)+0x364] FP: 0x66749270[etext(0x634036b4)+0x3345bbc], RA: 0x62E29614[cmm_notify_trigger(0x62e28e94)+0x780] FP: 0x66749320[etext(0x634036b4)+0x3345c6c], RA: 0x620A061C[OB_Setting_Alert(0x620a0570)+0xac] FP: 0x66749768[etext(0x634036b4)+0x33460b4], RA: 0x620D51E0[AFW_FSM_Drive(0x620d4ed8)+0x308] FP: 0x667497A8[etext(0x634036b4)+0x33460f4], RA: 0x620A1394[OB_FSM_Drive(0x620a12e8)+0xac] FP: 0x667497D0[etext(0x634036b4)+0x334611c], RA: 0x620AC074[AFW_M_Destination_Action(0x620abf10)+0x164] FP: 0x66749800[etext(0x634036b4)+0x334614c], RA: 0x6206D3AC[AFW_Module_Action(0x6206d2c8)+0xe4]

Workaround: There is no workaround.

Further Problem Description: Previous bug id CSCsr06874 fix applied.

- CSCsw67608

  Symptoms: No symptoms; needed for CSCso89298.

  Conditions: This is observed in Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsw70566

  Symptoms: User is experiencing port block when using STCAPP. Behavior is that when going offhook, no dialtone can be heard. Only performing a shut/no shut on the voice port can bring it back to IDLE and get the dialtone.

  Conditions: Customer is using CUCM and VG224 gateway to connect to analog phones. Skinny is the control protocol.

  Workaround: There is no workaround.

  Root Cause Analysis: Before PI9, the VPM layer will never send the disconnect confirmation and the setup_ind at the same time (or within 4 milliseconds). But after PI9, a ddts fix CSCsq97697 changed the behavior. In the case when the user goes onhook. Then, immediately after the hookflash duration is passed, he offhook the phone. Before PI9, this behavior will cause the new call's setup be postponed until the next time the user goes onhook. But now, the setup_ind of the new call will be immediately sent right after the previous call's disconnect confirmation. So, when messages traversed to VTSP layer, because of the nature of the DSMP dsp process, the disconnect_done event has more chance to come later than the new call's setup_ind.

  In STCAPP, our design is based on the behavior of the time when it was developed (PI2). So we do not handle that sequence. But now, since this is the behavior, we will have to handle that case when disconnect_done comes after the new call's setup_ind.

Fix and Unit Test: The fix is to enhance the disconnect_done handler to make it more robust and more fault tolerant to accommodate this situation.

Unit test is done and the results are passed.

- CSCsw71188

  Symptoms: A Cisco 7200 router loses connectivity to the SDH link. The same behavior has happened in several places.

  Topology:

  PPPoverATM ---- C7200 POS ---SDH---- ONS15454 ----- OPTICAL CLOUD ---- ONS 15454 ----SDH------- POS C12416

  Conditions:

  1. The C12416 receives a PAIS alarm from the optical network.

  2. The interface goes down and up, and the alarm is cleared from the C12416 side.

  3. The C7200 loses connectivity.

  4. The C12416 POS interface is still up, but pinging fails.

  5. After the interface was shut down and re-enabled, it was in serial up but protocol down. From C12416 side.

  6. Until the fiber was disconnected and reconnected from the C7200 side, the link was recovered.

  Workaround: Disconnect and re-connect the fibers from the C7200 side.

- CSCsw72677

  Symptoms: A router crashes with “no bba-group pppoe.”

  Conditions: This symptom happens after bba-group is unconfigured.

  Workaround: There is no workaround.

- CSCsw74836

  Symptoms: Enabling the **auto qos voip** command under an ATM PVC displays an error.

  Conditions: This symptom is observed with a Cisco 7200 router that is loaded with Cisco IOS Release 12.4(23.12)T.

  Workaround: There is no workaround.

- CSCsw76130

  Symptoms: A crash occurs because of a watchdog timer (CPU HOG).

  Conditions: This symptom is observed when "cns config initial" is used to download a large config (~ 20000 bytes) when “cns config notify diff” is also on.

  Workaround: Add “cns config notify diff” to the config after you have applied the initial config to the device.

- CSCsw78939

  Symptoms: No new sessions can come up using VPDN after a few days.

  Conditions: The root cause is that we leak and run out of SSM switch IDs.

  Workaround: There is no workaround.

- CSCsw80206

  Symptoms: Build failure for the Cisco 880 series.

  Conditions: This is a side effect of CSCsw72677.

Workaround: There is no workaround.

- CSCsw92379

  Symptoms: Many “IP ARP: Sticky ARP entry invalidated” syslog messages appear, and the RP reloads unexpectedly.

  Conditions: This symptom is observed when a linecard is swapped while thousands of DHCP snooping bindings are present and the **ip sticky-arp** command is configured.

  Workaround: Configure the **no ip sticky-arp** command.

- CSCsx28297

  Symptoms: While the **atm pvp** command is applied under the ATM interface, a router reloads.

  Conditions: This symptom is observed while the **atm pvp** command is applied under the ATM interface.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(20)T1

Cisco IOS Release 12.4(20)T1 is a rebuild release for Cisco IOS Release 12.4(20)T. The caveats in this section are resolved in Cisco IOS Release 12.4(20)T1 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCee21263

  Symptoms: Fragmented packets might be dropped by the router.

  Conditions: This is observed with non-initial fragments, when a reflexive ACL is configured on the router and the return traffic supposed to be allowed by the reflexive ACL is fragmented.

  Workaround: There is no workaround. However, normal ACLs are not known to exhibit this behavior.

- CSCek63963

  Symptoms: Router crashes with a traceback decode showing a divide by 0 error.

  Conditions: Occurs when a rate-based event is configured for a counter that has a value of 0, such as the following scenario:

  1. The customer must be using a Cisco IOS Embedded Event Manager (EEM) rate-based Interface Event Detector (either applet or Tcl script). Rate-based means use of the “rate” keyword in the event specification statement.

  2. The rate calculation is attempted after the counters are cleared and before any samples have been taken.

  Workaround: There is no workaround.

- CSCek64863

  Symptoms: DHCP Relay crashes while sending a DHCP offer to the client with binding as relay binding. (0.0.0.0).

  Conditions:

1. Client is either not sending the client-id option or sending the MAC address as the client-id option in all the DHCP messages toward DHCP Relay.

2. Either smart relay is configured on the relay or relay is unnumbered so that relay bindings get created on the router.

Workaround: Disable smart-relay functionality if enabled. Use numbered relay instead of unnumbered relay.

- CSCek71050

  Symptoms: Compared to other Cisco IOS software releases, unusually high CPU usage may occur in the BGP router process on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

  Conditions: This symptom is observed when BGP is learning routes from the RIB, even if redistribution is not directly configured under BGP. (Redistribution from other routing protocols to BGP can exacerbate the CPU usage.)

  Workaround: There is no workaround.

- CSCek74114

  Symptoms: ASL Rollback was not able to remove ASL configuration **configuration mode exclusive auto lock-show** from the running-config.

  Conditions: Failure is seen using ASL Rollback on Cisco 7600.

  Workaround: There is no workaround.

- CSCek75558

  Symptoms: When hardware compression is enabled and an MQC policy is used on an FR PVC, the shaper drops all packets after passing a few.

  Conditions: This symptom is observed with normal traffic flow through the interface.

  Workaround: Replace MQC shaping with FRTS and configure the shape rates in the map class. If LLQ is not required on the PVC, another option is to use software compression instead of hardware compression.

- CSCsc72722

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

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

  Workaround: There is no workaround.

- CSCsg15342

  Cisco 10000, uBR10012 and uBR7200 series devices use a User Datagram Protocol (UDP) based Inter-Process Communication (IPC) channel that is externally reachable. An attacker could exploit this vulnerability to cause a denial of service (DoS) condition on affected devices. No other platforms are affected.

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

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

- CSCsg99677

  Symptoms: Crashinfo collection to a disk filesystem will fail and generate the following error message:

```
File disk#:crashinfo_20070418-172833-UTC open failed (-1): Directory entries are
corrupted, please format the disk
```

Or the crashinfo file will be stored as CRASHI~1.

Conditions: This symptom is observed with normal crashinfo collection to a disk filesystem.

Workaround: Configure the crashinfo collection either to a network filesystem (such as tftp or ftp) or to a local filesystem of type “flash”. Configuring to a local filesystem is a preferable option.

Further Problem Description: This happens every time, but there is no major negative impact to operation.

- CSCsh66406

  Symptoms: When you enter the **maximum route x y** VRF configuration command or reduce the *limit* argument of the **maximum route** VRF configuration command, stale routes may occur in the BGP VPNv4 table.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the connection with a CE router is configured for another protocol than BGP such as OSPF and when the routes are redistributed into BGP.

  Impacts: May have functional impact.

  Trigger: The **maximum route x y** VRF configuration command.

  Workaround: If OSPF is the other protocol, enter the **redistribute ospf** address-family configuration command.

- CSCsi51014

  Symptoms: Disk access causes router to crash.

  Conditions: Occurs after **fsck** execution.

  Workaround: Format disk, which causes the data loss on the affected disk.

- CSCsj49293

  Symptoms: The interface output rate (214 Mb/s) is greater than the interface line rate (155 Mb/s).

  Conditions: This symptom is observed with a Cisco 7600/7500/7200-NPE400 and below. That is, PA-POS-2OC3/1OC3 (PULL mode).

  Workaround: There is no workaround.

  Further Problem Description: From the Ixia, packets are transmitted at 320 Mb/s. On the UUT (Cisco 7600), the outgoing interface (POS-Enhanced Flexwan) shows the output rate as 200 Mb/s. But the interface bandwidth is 155 Mb/s.

- CSCsk05653

  Symptoms: The **aaa group server radius** subcommand **ip radius source-interface** will cause the standby to fail to sync.

```
c10k-6(config)# aaa group server radius RSIM
c10k-6(config-sg-radius)# ip radius source-interface GigabitEthernet6/0/0
c10k-6# hw-module standby-cpu reset
c10k-6#
Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT) Aug 13 14:49:31.793 PDT: %C10K_ALARM-6-INFO: ASSERT MAJOR RP A
Secondary removed Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby
processor fault (PEER_DOWN) Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST:
Standby processor fault (PEER_REDUNDANCY_STATE_CHANGE) Aug 13 14:49:31.793 PDT:
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT) Aug 13
14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN) Aug
13 14:49:31.813 PDT: %REDUNDANCY-3-IPC: cannot open standby port no such port Aug 13
```

```
14:49:32.117 PDT: %RED-5-REDCHANGE: PRE B now Non-participant(0x1C11 => 0x1421) Aug 13
14:49:32.117 PDT: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby
insertion (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
Aug 13 14:50:52.617 PDT: %RED-5-REDCHANGE: PRE B now Standby(0x1421 => 0x1411) Aug 13
14:50:54.113 PDT: %C10K_ALARM-6-INFO: CLEAR MAJOR RP A Secondary removed Aug 13
14:51:33.822 PDT: -Traceback= 415C75D8 4019FB1C 40694770 4069475C Aug 13 14:51:33.822
PDT: CONFIG SYNC: Images are same and incompatible
Aug 13 14:51:33.822 PDT: %ISSU-3-INCOMPATIBLE_PEER_UID: Image running on peer uid (2)
is the same -Traceback= 415CCC2C 415C75FC 4019FB1C 40694770 4069475C Aug 13
14:51:33.822 PDT: Config Sync: Bulk-sync failure due to Servicing Incompatibility.
Please check full list of mismatched commands via: show issu config-sync failures mcl
Aug 13 14:51:33.822 PDT: Config Sync: Starting lines from MCL file: aaa group server
radius RSIM ! <submode> "sg-radius" - ip radius source-interface GigabitEthernet6/0/0
```

Conditions: This symptom is observed if the **aaa group server radius** subcommand **ip radius source-interface** CLI is configured on a box with dual PREs.

Workaround: If the customer does not use the **aaa group server radius** subcommand **ip radius source-interface** *interface*, this will not be a problem.

If they use the **aaa group server radius** subcommand **ip radius source-interface** *interface* on a Cisco 10000 router in simplex mode (a single PRE), this will not be a problem.

If they run with dual PREs, then they will need to remove the **aaa group server radius** subcommand **ip radius source- interface** *interface* from the configuration as a workaround.

Removing the **aaa group server radius** subcommand **ip radius source-interface** *interface* from the configuration could cause problems for the customer. The radius server may be expecting the request to come from a specific source address. The router will now use the address of the interface the packet egresses the router from, which may change over time as routes fluctuate.

- CSCsk06777

  Symptoms: Firewall may inspect traffic that is denied by output ACL.

  Conditions: Occurs when firewall and ACL are applied in the same direction on output interface.

  Workaround: There is no workaround.

- CSCsk28361

  Symptoms: 4000 virtual-template (VT) takes high CPU during system load configuration.

  Conditions: Occurs when 4000 VT interfaces are loaded from TFTP to running configuration.

  Workaround: There is no workaround.

- CSCsk39308

  Symptoms: An asynchronous interface cannot successfully be configured as **ip unnumbered** to a loopback interface.

  Conditions: Occurs with the following configuration:

  Router(config)# interface Group-Async1

  Router(config-if)# ip unnumbered Loopback0

  Point-to-point (non-multi-access) interfaces only

  Workaround: There is no workaround.

- CSCsk44568

  Symptoms: Counters on input interface and receivers interface are not in sync when rate-limit is applied on input interface.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(16.14)T4 with rate-limit configured on input side.

Workaround: There is no workaround.

- CSCsk65460

  Symptoms: Multicast fast switching fails on the decapsulating provider edge (PE) router when encryption is configured.

  Conditions: This symptom is observed on a Cisco 7200 router with Cisco IOS Release 12.4(17.4)T1.

  Workaround: There is no workaround.

- CSCsk76053

  Symptoms: When using route-map to redirect the traffic from one physical interface to be rerouted to the loopback interface, the traffic is not redirected.

  Conditions: This symptom is observed when the router is configured for “EZvpn client on stick” 1interface inside/outside, loop being the inside.

  Workaround: Configure interface vlan1.

- CSCsl44498

  Symptoms: Serial interface (CT1) goes down when attaching a policy with traffic and a class map that has an extended ACL.

  Conditions: Occurred on a Cisco 7200 Router with extended ACL with traffic.

  Workaround: There is no workaround.

- CSCsl51353

  Symptom: The packets are getting dropped on the ATM subinterface.

  Conditions: Occurs when shaping is configured in the policy-map. Enable cef on the router, apply service-policy on the ATM interface of the router and send traffic. Now check for the packets count on the router. Packets will be getting dropped.

  Workaround: There is no workaround.

  Further Problem Description: This issue manifests packet drops even in absence of congestion when a service policy configured with any shaping feature is attached to an ATM interface.

- CSCsl97384

  Symptoms: Router reload is seen in the network with a traceback when the **show aaa user all** command is executed.

  Conditions: This symptom occurs when the command is executed with 2000 or more sessions in progress.

  Workaround: Do not enter the **show aaa user all** command.

  Further Problem Description: This is more like a timing or race condition, which could occur with a large number of sessions.

  The **show** command outputs data from General DataBase which is typically a hash table for each session. However, it does not lock the table during the display for each session. When we have a large number of sessions, the output process may take more than one pass. Meantime if we clear the session, we free the memory associated with that session’s General DB. Now, pointers the **show** command is using, point to a freed memory resulting in a reference to a bad pointer. The output process has to sleep (suspend) a moment, and the crash occurs.

- CSCsl99275

  Symptoms: High CPU can be seen on a Cisco AS5400XM after a certain uptime.

Conditions: Occurs after 2 to 3 weeks of uptime. CPU usage increases because of “Background Loade” process.

Workaround: Reload the access server.

- CSCsm13968

  Symptoms: A router crashes when a service policy with FPM is configured, removed, and reconfigured on an interface.

  Conditions: This symptom is seen only when the service policy is configured, then removed, and reconfigured on the same or a different interface.

  Workaround: There is no workaround.

- CSCsm21335

  Symptoms: When the **cm-manager config server** *ip-address* command is used, the router fails to configure or misconfigures the gateway voice ports. This results in non-functional voice ports.

  Conditions: Occurred on a Cisco 3845 running the c3845-advipservicesk9-mz.124-13d.bin image. Example of the errors follow:

  voice-port 1/0/0 signal unknown <--- should have been default loop start ring frequency unknown <--- should have been default ring freq timing hookflash-in 400 20 shutdown <--- should have been no shut

  In addition, PRI E1 trunks fail with no dial tone yet there is no indication why. The Cisco IOS configuration looks OK.

  Workaround: Do not use these commands. Configure the MGCP gateway manually.

- CSCsm34226

  Symptoms: Router crashed during stress test of 5000 to 6000 56-byte UDP packets per second.

  Conditions: Occurred on a Cisco 878 router running Cisco IOS Release 12.4(15)T1.

  Workaround: There is no workaround.

- CSCsm48357

  Symptoms: When FlexWAN card configured for Frame Relay over MPLS (FRoMPLS) is subjected to online insertion and removal (OIR), the standby will crash when FRoMPLS is unconfigured.

  Conditions: Occurs when FRoMPLS is unconfigured following an OIR.

  Workaround: There is no workaround.

- CSCsm57494

  Symptoms: BGP update is not sent after reloading opposite router or resetting module. Sometimes a BGP VPNv4 label mismatch also occurs between the routers because BGP update is not received.

  Conditions:

  – This problem may occur once or twice out of 20 attempts.
  – This problem is apt to occur when MPLS-TE tunnel is enabled.
  – This problem may occur when entering either **reload** command, **hw-module module X reset** command or the **clear ip bgp X.X.X.X** command on the opposite router.

  Workaround: There is no workaround.

- CSCsm73592

  Symptoms: A reload may occur when an anything over MPLS (AToM) VC is torn down. Bug triggered initial crash of SIP-400 in slot 4 & ES20 in slot 3. Both cards had to be powered down and reset from the console to recover.

  Conditions: Occurs when AToM VC is setup and torn down later.

  Workaround: There is no workaround.

  Further Problem Description: The crash may occur when an event triggers access to a previously set up AToM VC. For example, the crash may occur when fast reroute (FRR) is configured on the tunnel interface and the primary interface is removed, such as in the following scenario:

```
pseudowire-class ER1_to_HR1_EoMPLS
 no preferred-path interface Tunnel501331 disable-fallback
!
interface tunnel501331
 shutdown
!
no interface tunnel501331
```

- CSCsm73602

  Symptoms: High CPU load due to VTEMPLATE Backgr process.

  Conditions: Occurs when **ip multicast boundary** command is used on many interfaces (8000 or more).

  Workaround: There is no workaround.

- CSCsm75286

  Symptoms: A route-map that is configured with both IPv4 and IPv6 for a BGP peer does not work as expected.

  Conditions: Observed after the route-map is modified to delete a sequence.

  Workaround: Apply a fresh route-map.

- CSCsm85249

  Symptoms: Mobile IP (MoIP) tunnel never comes up on a mobile router when roaming to the cellular interface. This is because the HWIC-3G-GSM never receives or accepts the registration reply from the Home Agent.

  Conditions: Occurred on a Cisco 3845 router.

  Workaround: There is no workaround.

- CSCsm87884

  Symptoms: During performance testing, a 20-percent CPU utilization increase is noticed between Cisco IOS Release 12.4(9)T7 and Release 12.4(15)T3. The increase in CPU utilization is seen with 300 byte cos2, cos3, and cos4 traffic only.

  Conditions: The symptom is observed when QoS is configured on the router. It is seen with Cisco IOS Release 12.4(15)T and may also apply to Cisco IOS Release 12.4(11)T.

  Workaround: There is no workaround.

- CSCsm89795

  Symptoms: The router keeps reloading and complaining about unavailability of memory.

  Conditions: This symptom is observed if the router is directly connected to a DHCP server or if an attack is made by flooding DHCP replies.

  Workaround: There is no workaround.

- CSCso00383

  Symptoms: Multicast VPN scenario may not work due missing Border Gateway Protocol (BGP) multicast distribution tree (MDT) Route Distinguisher (RD) type 2 updates not being sent by provider edge (PE) supporting new style updates (IPv4 MDT address-family).

  Conditions: Issue is seen on Catalyst 6000 series switch running Cisco IOS Release 12.2(33)SXH1.

  Workaround: There is no workaround.

- CSCso01307

  Symptoms: On a Hot Standby Router Protocol (HSRP) standby router, all accounting records for **aaa accounting commands** and **aaa accounting system** on the standby router of the HSRP pair are available only if those two commands are applied.

  Conditions: AAA accounting is configured on a router pair that is running HSRP.

  Workaround: Change the router to the active state before making changes that are to be logged.

  Further Problem Description: The following message will appear when the **debug aaa accounting** command is executed and a record is suppressed:

  ```
  *<time/date>: AAA/ACCT/CMD(00000003): Suppressed record
  ```

- CSCso02348

  This is an enhancement request to add more description to the OER fields. Right now it is very hard to follow unless you are familiar with the command.

- CSCso12305

  Symptoms: The IPv6 Cisco Express Forwarding (CEF) table may be missing prefixes which are present in the IPv6 RIB.

  Conditions: Occurs when CEF is disabled and re-enabled.

  Workaround: Enter the **clear ipv6 route *** command.

- CSCso13102

  Symptoms: Configuring a QoS policy, including Control Plane Protection (CPPr) and Control Plane Policing (CoPP), using ACLs with overlapping ACEs can cause ACEs to be skipped or processed out of order.

  Conditions: When ACLs are used with CPPr, CoPP, or standard QoS policies, ACEs may be skipped when examining traffic that may match more than one ACE. For example, the following ACL is used with a CPPr configuration that is applied to the aggregate control-plane interface.

  ```
  access-list 110 deny icmp host 192.168.100.1 any
  access-list 110 permit icmp host 192.168.100.1 any
  access-list 110 deny icmp any any
  access-list 110 permit icmp any any
  ```

  Sending pings from 192.168.100.1 to 10.255.255.102 results in the following **show access-list** output, and the incoming pings are in fact dropped.

  ```
  Router# show access-list

  Extended IP access list 110
       10 deny icmp host 192.168.100.1 any
       20 permit icmp host 192.168.100.1 any (11 matches)
       30 deny icmp any any
       40 permit icmp any any (5 matches)
  ```

  Workaround: Remove overlapping ACE entries or rework the ACL.

- CSCso19662

  Symptoms: Tracebacks are seen after unconfiguration when using the **clear ip nat translation *** command.

  Conditions: This traceback occurs with the c7200-js-mz.124-18a.fc2 image.

  Workaround: There is no workaround.

- CSCso21888

  Symptoms: Router may spontaneously reload.

  Conditions: Occurs on routers configured with iSPF computation algorithm in OSPF.

  Workaround: Disable iSPF.

- CSCso28309

  Symptoms: Ping fails from reflector during internal testing.

  Conditions: The goal of the test is to verify the successful termination of PPP/PPPoE over ATM sessions on router's ATM interface using auto sensing. It is performed with auth_pap, process switch, and keepalive disabled. This has a functional impact as the virtual access entry is not getting added to the routing table after doing clear ip route.

  Workaround: There is no workaround.

- CSCso39886

  Symptoms: A router crashes when PPPoE sessions are coming up.

  Conditions: This symptom is observed on a Cisco 7301 router when QoS policing is applied to the PPPoE sessions.

  Workaround: There is no workaround.

- CSCso41513

  Symptoms: When using the **ip helper-address** command to forward directed broadcast, an incomplete ARP entry will be created for the helper-address configured even if it is not a directly connected subnet. This may break BOOTP forwarding to the DHCP server.

  Conditions: The symptoms are observed in Cisco IOS Release 12.4(19) only. Cisco IOS Release 12.4(18) does not have this issue.

  Workaround: Configure proxy-arp on the next hop device on the path to the DHCP server.

  Alternate Workaround: Configure static ARP on the router for the helper-address pointing toward the next hop.

- CSCso47048

  Symptoms: A router may crash with the following error message:

  ```
  %SYS-2-CHUNKBADFREEMAGIC: Bad free magic number in chunk header, chunk 6DF6E48 data
  6DF7B48 chunk_freemagic EF430000 -Process= "Check heaps", ipl= 0, pid= 5,
  -Traceback= 0x140C170 0x1E878 0x1EA24 0x1B4AC 0x717DB8 chunk_diagnose, code = 2 chunk
  name is PPTP: pptp_swi
  current chunk header = 0x06DF7B38 data check, ptr = 0x06DF7B48
  next chunk header = 0x06DF7B70 data check, ptr = 0x06DF7B80
  previous chunk header = 0x06DF7B00 data check, ptr = 0x06DF7B10
  ```

  Conditions: Issue has been seen on Cisco 7200 router with NPE-G2 configured for L2TP and running Cisco IOS Release 12.4(15)T3 and Cisco IOS Release 12.4(15)T4.

  Workaround: There is no workaround.

- CSCso51749

  Symptoms: QoS works fine with unicast packets over a GRE tunnel, but it does not work for multicast over GRE tunnels.

  Conditions:

  1. Apply a simple policing policy on a GRE tunnel.

  2. Build an mroute table entry.

  3. Send multicast traffic switched over the tunnel.

  4. Verify the police functionality.

  Workaround: There is no workaround.

- CSCso52344

  Symptoms: On an RP, the **show ip cef** command displays the nexthop as drop for the 224.0.0.0/4 prefix, but on the linecard the nexthop is displayed as multicast.

  Conditions: This issue occurs when **ip multicast-routing** is not configured and when the command **show ip cef** is issued on the RP and linecard.

  Workaround: There is no workaround.

  Further Problem Description: This is a cosmetic issue.

- CSCso52837

  Symptoms: While executing the **copy run disk0:test** command, the following error is received:

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

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

  Workaround: Use a "/", as in **copy run disk0:/test**.

- CSCso60063

  Symptoms: Router crashes when the **no password pass** command is issued from the console while configuring the **dot1x credentials** command in configuration mode.

  Conditions: Occurs only when the **no password pass1** command is entered.

  Workaround: There is no workaround.

- CSCso62166

  Symptoms: Device crashes while debugging Border Gateway Protocol (BGP) IPv6 unicast updates entering the **clear bgp ipv6 uni *** command.

  Conditions: Debugging must be on to see the crash.

  Workaround: Use the **no debug bgp ipv6 unicast update** command to turn off BGP IPv6 unicast updates debugging.

- CSCso62266

  Symptoms: Router forwards Bridge Protocol Data Unit (BPDU) after disabling spanning-tree. But after reload, it blocks the BPDU.

  Conditions: Occurs when switch-port is configured.

  Workaround: Enable spanning-tree. You may then disable it again if it is not desired.

- CSCso63263

  Symptoms: The RP will start showing IPC-5-WATERMARK: 988 messages pending in xmt for the port messages on the screen. The number of messages will change.

Conditions: The router has 275,000 i-BGP routes injected into the router. Among these routes, 100,000 are flapped continuously for one to one and half days. They are flapped every 10 sec. The problem needs at least a days worth of time of continuous flapping.

Workaround: Stop the route flap. Although the messages will keep coming, there is no impact on functionality. And they are bogus since they are originated from wrong count.

- CSCso64104

  Symptoms: A router may crash after applying the configurations related to PA- MC-2T3-EC immediately after the router reloads.

  Conditions: The symptom is observed on Cisco 7200 series and a 7301 router.

  Workaround: Do not configure PA-MC-2T3-EC immediately after the router reloads.

- CSCso64607

  Symptoms: A router may crash when the **no ip vrf** command is issued.

  Conditions: The symptom occurs when VRF was previously configured on a tunnel interface that has subsequently been removed.

  Workaround: Possibly unconfigure the **ip vrf** command before unconfiguring the tunnel interface.

- CSCso64889

  Symptoms: A router log contains the following error message, and its performance becomes severely degraded:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs 4/3),process =
  DNS Server.
  ```

  Conditions: This symptom is observed on a Cisco router that performs many DNS lookups.

  Trigger: This symptom occurs when there are many DNS lookups, but it may also occur otherwise.

  Impact: This bug impacts performance.

  Workaround: Configure the router in such a way to prevent it from performing many DNS lookups, and do not configure the router as a DNS server for other devices.

  Further Problem Description: Note that CSCsg64586 can produce very similar symptoms, even in the absence of a large number of DNS queries.

- CSCso65193

  Symptoms: The memory occupied by the IP SLA Event Processor may gradually increase.

  Conditions: The issue occurs when IP SLA jitter operation is configured on the router without source port specification.

  Workaround: There is no workaround.

  Further Problem Description: With 1000 IP SLAs configured (200 each of following types: path-echo, path-jitter, icmp-echo, udp-jitter and udp-echo, each with a unique destination), the memory allocated for “IP SLAs Event Pr” increases and the level of available processor memory goes down. This issue will have a performance impact.

- CSCso66396

  Symptoms: If the dialing process is interrupted with a Carrier Drop message, it is not possible to attempt a new call for that remote site.

  Conditions: After receiving a Carrier Drop message, the dialer is not cleared. The **show dialer session** command reports status 6 for that call. Traffic directed to the remote site is dropped. The dialer map is still active. All the traffic is still routed to the dialer and dropped.

  Workaround: Clear the dialer session.

Further Problem Description: This will impact traffic forwarding.

- CSCso66473

  Symptoms: A router may crash when the user moves from one segment to another and attempts to log onto SSG.

  Conditions: The symptom is observed in the following situation:

  1. Open a user known to SSG through accounting-start with an IP address of “IP1.”

  2. User then logs onto SSG.

  3. User moves to another segment which generates another accounting-start for the same MAC address but a different IP address, IP2.

  4. The SSG then crashes.

  Workaround: There is no workaround.

- CSCso73533

  Symptoms: Traceback is seen after unconfiguring the tunnel interface.

  Conditions: The symptom is seen when using Ipv4 multicast PIM tunnels where the route to the Rendez-Vous Point (RP) is via another tunnel interface. If this tunnel interface was unconfigured, then there is a race condition between: 1. learning about the new route to the RP via another interface; and 2. periodic update of the PIM tunnel adjacency. If the latter occurs first the traceback is seen.

  Workaround: There is no workaround.

- CSCso78897

  Symptoms: A Cisco 870 router will process and forward packets received with a multicast MAC address even though it should not, such as when the interface controller does not own the multicast MAC address.

  Conditions: This was observed on a Cisco 878 Router running Cisco IOS Release 12.4(15)T4.

  Workaround: Make sure the switch connecting to the Cisco 870 does not send packets with multicast MAC addresses that should not be received by the Cisco 870.

- CSCso80288

  Symptoms: The value of AOC is missing for the Release Message.

  Conditions: The symptom is seen for switch type basic-net3. It occurs when configuring OGW and TGW with the **isdn global-disconnect** command.

  Workaround: There is no workaround.

- CSCso81854

  Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

  To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080708-dns.shtml.

This security advisory is being published simultaneously with announcements from other affected organizations.

- CSCso82469

  Symptoms: If a user tries to create new mail, the OWA displays an improper message (such as the page cannot be displayed or that the page cannot be loaded) and the OWA session hangs. This will cause the rest of the session to be unresponsive to any more connections.

  Conditions: The symptom is observed on a server configured with the OWA feature. The issue only occurs when trying to access OWA.

  Workaround: There is no workaround.

- CSCso82732

  Symptoms: Every hour (at 31 minutes past the hour), three to six calls fail. The cause is given as "cause 47" (resource not available) and "cause 16" (cause 16 errors usually follow cause 47 errors).

  Conditions: The symptoms are observed every hour under load conditions when 20 or more T1 channels are turned on. No errors are seen with a load less than 20 channels.

  Workaround: Use Cisco IOS Release 12.4(15)T5. Alternatively, remove the NTP configuration from the GK.

  Further Problem Description: CPU spikes are seen at the time of failures on NTP process. There are no call failures if the NTP configuration is removed.

- CSCso87348

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly.

  Conditions: Occurs when NetFlow is configured on one of the following:

  - Cisco 7600 running Cisco IOS Release 12.2(33)SRC.
  - Catalyst 6500 running Cisco IOS Release 12.2SXH.

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

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

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

- CSCso88429

  Symptoms: CME or CUBE will reject an inbound SIP INVITE if Max-Forwards is greater than 70.

  Conditions: The symptoms are observed when a Max-Forwards header field in SIP INVITE is greater than 70.

  Workaround: There is no workaround.

  Further Problem Description: From RFC 3261: 20.22 Max-Forwards

  The Max-Forwards header field must be used with any SIP method to limit the number of proxies or gateways that can forward the request to the next downstream server. This can also be useful when the client is attempting to trace a request chain that appears to be failing or looping in mid-chain.

  The Max-Forwards value is an integer in the range 0-255 indicating the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request. The recommended initial value is 70.

  This header field should be inserted by elements that can not otherwise guarantee loop detection. For example, a B2BUA should insert a Max-Forwards header field.

- CSCso91078

  Symptoms: A Cisco IAD2430 may reload unexpectedly because of a bus error (Sig=10).

  Conditions: The symptom is observed on a Cisco IAD2430.

  Workaround: There is no workaround.

- CSCso91341

  Symptoms: The following operations are legal but are rejected on the grounds that there is insufficient bandwidth: 1. A QoS policy-map is attached as a service-policy to an interface or other valid target; or 2. A previously attached policy-map is modified.

  Conditions: The symptoms are observed when, prior to the error, a policy-map failed to be attached or modified due to insufficient bandwidth to meet the bandwidth guarantees in the policy-map.

  Workaround: Remove all policy-maps from the affected target. Attach a simple policy-map with no bandwidth guarantees (e.g., having only a **shape** command). Remove this service-policy. This should remove all queueing data structures from the target. Proceed to attach the original policy-map.

- CSCso92175

  Symptoms: The configured value of a queue-limit gets changed and locked at 16000 bytes when random-detect is applied to the policy-map and service policy is attached to the interface.

  Conditions: The symptom is observed when a queue-limit is configured in front of the WRED in the same class of policy-map.

  Workaround: Configure the WRED in front of queue-limit in the same class of policy-map.

- CSCso93065

  Symptoms: Standby RP crashes while receiving dynamic sync from active RP during DHCP relay binding creation.

  Conditions: Occurs when the router is configured as DHCP relay and is running Cisco IOS images that include the fix for CSCsm86039.

  Workaround: There is no workaround.

- CSCso93867

  Symptoms: Router crashes with bus error exception.

  Conditions: This happens when **qos service-policy** is unconfigured or reconfigured on a virtual-template interface.

  Workaround: There is no workaround.

- CSCso95136

  Symptoms: Cisco 181x series router crashes.

  Conditions: Occurs while unconfiguring dialer in band on asynchronous interface.

  Workaround: There is no workaround.

- CSCso96729

  Symptoms: The Cisco 88x voice and data routers occasionally crash during Cisco IOS boot up.

  Conditions: The crash occurs after power cycling the router several hundred times. The router crashes during the booting of Cisco IOS. Depending on the configuration register, the router will reboot itself and run normally.

  Workaround: Upgrade the ROMMON version to Version 12.4(15r)XZ5.

- CSCso97593

  Symptoms: Cisco ASR1000 loses QoS configuration after reload.

  Conditions: Cisco ASR1000 will lose the configuration if flat service policy is configured on Multilink Point-to-Point Protocol (MLPPP) bundles.

  Workaround: This problem is not seen if MLPPP bundles are configured with hierarchical service policy.

- CSCso98430

  Symptoms: A PPPoE session fails to come up.

  Conditions: This symptom is observed on a Cisco router loaded with Cisco IOS Release 12.4T, and when virtual-template is configured.

  Workaround: There is no workaround.

- CSCsq01531

  Symptoms: UC520 took software exceptions.

  Conditions: When a client calls to IXI interface.

  Workaround: There is no workaround.

- CSCsq02771

  Symptoms: DHCP relay may hang when request for IP address is received from a DHCP client on an unnumbered in an MPLS and VPN setup.

  Conditions: The symptom is observed on a Cisco 7200 router that is running Cisco IOS Interim Release 12.4(19.16)T1.

  Workaround: There is no workaround.

- CSCsq03005

  Symptoms: Fax fails when the **supervisory disconnect** command is applied on a voice port. The default fax detect script, app_fax_detect.2.1.2.2.tcl, is being used.

  voice-port 2/0/20
  supervisory disconnect dualtone mid-call

  When the **supervisory disconnect dualtone mid-call** command is removed, fax works.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T4.

  Workaround: There is no workaround.

- CSCsq03115

  Symptoms: The PIM configuration may be missing and the following traceback is seen:

  ```
  %SYS-3-MGDTIMER: Running timer, init, timer = 895661C. -Process= "Exec", ipl= 0, pid=
  80, -Traceback= 0x14C0F30 0x31DA638 0x31DA7C8 0x31DA914 0x1E019B4 0x1E35634 0x1E34AD0
  0x15160F8 0x1515234 0x1542208 0x695548
  ```

  Conditions: The symptom is observed symptom is observed after performing an OIR of the PA-T3+ serial port adapter. The symptom occurs twice.

  Workaround: Reconfigure the PIM mode.

- CSCsq05997

  Symptoms: The following error messages may appear in the log file multiple times:

  ```
  %ARP-3-ARPINT: ARP table accessed at interrupt level 1, -Traceback= 0x61013944
  0x60B61F80 0x60B5A2A4 0x6019DDAC 0x600FA37C 0x600FCC6C
  ```

  Because the message is generated frequently, the log file may fill up too soon.

Conditions: The symptom is observed because a Cisco IOS component is accessing the ARP cache table in the interrupt context, which against the design of the Cisco IOS module. The error message indicates that the software is in danger of causing the router to crash.

Workaround: There is no workaround.

- CSCsq06645

  Symptoms: Packets may get dropped when a route map is applied to peergroup members.

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4T. The problem is seen when the combination of peergroup and route map is used.

  Workaround: There is no workaround.

- CSCsq06813

  Symptoms: Only one RELEASE message is seen on a DHCPv6 when the server is shut, even though multiple messages are expected.

  Conditions: The symptom occurs on Cisco 7200 series router that is running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsq09592

  Symptoms: The router is black-holing traffic that is going to be encrypted. The crypto-counters are not showing an increase.

  Conditions: The symptoms are observed when service-policy is configured on the main interface and crypto map is configured on a subinterface and when IP CEF is enabled.

  Workaround: Redesign the configuration to apply service policy on the subinterface. Disable CEF globally.

  Further Problem Description: Clear text-traffic is effectively received by the router. It triggers the creation of Phase I/Phase II. However, it then appears to be blackholed:

```
interface Ethernet0/0
 no ip address
 service-policy output shape
!
interface Ethernet0/0.10
 encapsulation dot1Q 10
 ip address 10.0.0.1 255.255.255.252
 crypto map mymap
```

- CSCsq09836

  Symptoms:

  1. For some Cisco 3660 platform images, the **connect** command is not working and as a result local switching does not work.

  2. For some images, the **no connect** command is not working to remove an existing connection.

  Conditions: The symptoms are observed with Cisco 3660 platform images where both ac_atm and atm_switching subsystems are responsible for local switching.

  Workaround: Remove ac_atm and use only atm_switching for local switching.

  Further Problem Description: Problems may arise for other Cisco 3660 platform images having both ac_atm and atm_switching.

- CSCsq09942

  Symptoms: NM-CEM-4TE1 modules installed in Cisco 3845 routers running 12.4(11)T or 12.4(15T)3 codes with nine TS CEM groups configured have alignment issues. When the issue occurs, all **show cem** commands do not show any problems with the cards or CEM groups.

  Conditions: This symptom is observed on an NM-CEM-4TE1 module installed in Cisco 3845 routers with nine TS groups configured and connected to another vendor's PBX.

  Workaround:

  1. Shut/no shut the CEM group on either side. This fixes the issue temporally.

  2. Change the CEM group configuration to have one TS per CEM group.

  Further Problem Description: The issue can be observed with more details using a WAN analyzer between the CEM card and the PBX. There you can see that the traffic is entering through a specific TS and leaving through a different TS.

- CSCsq10730

  Symptoms: A Cisco router may display the following messages after enabling the advanced signature set in IOS-IPS:

  ```
  Too many UUIDs in pdu type 0x0E
  Too many UUIDs in pdu type 0x0B
  Too many UUIDs in pdu type 0x0E
  Too many UUIDs in pdu type 0x0B
  ```

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(15)T, that is utilizing Cisco IOS IPS v5 feature, and is running with the advanced signature set (MSRPC). Symptom occurs when incoming MSRPC packets are malformed or do not comply with protocol.

  Workaround: There is no workaround. The message is informational (cosmetic).

- CSCsq11620

  Symptoms: String handling is incorrect in the code which uses "strncpy" and "sprintf".

  Conditions: The symptoms are observed when accessing a specific string.

  Workaround: There is no workaround.

- CSCsq11750

  Symptoms: A Cisco router may crash when the **no mgcp** and the **no mgcp profile** *profile-name* commands are issued from the VTY, and the command **call- agent** *ip-address* is configured through the console in "config- mgcp-profile" mode.

  Conditions: The symptom is observed when there is simultaneous operation between the console line and the VTY line.

  Workaround: Configure using a single telnet connection instead of two.

- CSCsq12128

  Symptoms: If the WAN connection is DOWN on the VGW, the Media Gateway Control Protocol (MGCP) fallback mode may not load. The gateway remains in "MGCP Fallback mode: Enabled/OFF" mode.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(16).

  Workaround: Shut down the interface.

  Further Problem Description: It is possible that the link goes up and down frequently. The call manager application tries to download the XML file from CCM+TFTP even when the link is down. This sets a flag. The flag prevents the fallback.

- CSCsq12337

  Symptoms: Parsing of a SIP message with MIME content fails, which causes call termination.

  Conditions: The symptoms are seen when the SIP message contains application/qsig or application/x-q931 contents in MIME without a Content- Length SDP header.

  Workaround: Add a Content-Length SDP header for application/qsig or application/x-q931 contents with appropriate value. Alternatively, disable sending application/qsig or application/x-q931 contents in the SIP message.

- CSCsq13348

  The Cisco IOS Intrusion Prevention System (IPS) feature contains a vulnerability in the processing of certain IPS signatures that use the SERVICE.DNS engine. This vulnerability may cause a router to crash or hang, resulting in a denial of service condition.

  Cisco has released free software updates that address this vulnerability. There is a workaround for this vulnerability.

  NOTE: This vulnerability is not related in any way to CVE-2008-1447 - Cache poisoning attacks. Cisco Systems has published a Cisco Security Advisory for that vulnerability, which can be found at http://www.cisco.com/en/US/products/products_security_advisory09186a00809c2168.shtml.

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

- CSCsq14031

  Symptoms: Unable to ping IP address of session target. Packets of certain sizes (between 57 and ~63 bytes, depending on the type of packet) are corrupted when using a tunnel over a PPP multilink interface. EIGRP packets were within this range and so were dropped and caused the route to the IP address being pinged not to be added.

  Conditions: Issue may be related to encryption or Network Address Translation (NAT).

  Workaround: Disable or increase the value of the **ppp multilink fragmentation** command.

- CSCsq14210

  Symptoms: A router may crash when a ping is issued and when the **clear ip cef * prefix-statistics** command is issued on router.

  Conditions: The symptom is observed when encapsulation FR is configured on the dialer interface, having profile configuration, and CEF switching is also configured.

  Workaround: There is no workaround.

  Further Problem Description: When encapsulation FR is configured on the dialer interface having profile configuration, it was made as a CEF switchable interface by default. When the CEF looks for a fastsend vector, the vector was NULL and router crashes at this point. Encapsulation ppp has its own way of installing the punt adjacency when the call is not UP and then it makes the interface a CEF switchable interface when the call comes UP.

- CSCsq15496

  Symptoms: Auto-Upgrade Manager (AUM) crashes while downloading an ipbase image.

  Conditions: This symptom is observed when AUM is used to download an ipbase image.

  Workaround: An upgrade to an ipbase image can be done without using AUM. Use the manual method of upgrading to a new image.

- CSCsq15560

  Symptoms: In creating a multi-party video conference by calling into a Cisco IPVC MCU device, a call may intermittently suffer from one-way video.

Conditions: The symptom is seen with a multi-party video conference which calls into a Cisco IPVC MCU device and where a local CME video endpoints calls the MCU via a gatekeeper over H323. This is a timing issue in the H.323 state machine. In a call flow, two sets of OLCs (for audio and video) are exchanged. BRQ is sent for audio OLC. Before BCF is received, GW gets video OLC. This updates the total channel bandwidth and checks if it is less then the approved BW. As it is not so, OLC is rejected resulting in one-way video.

Workaround: There is no workaround.

Further Problem Description: This scenario works fine with third party H323 endpoints with their own H323 stacks working with the same gatekeeper and MCU. A more heavily loaded (for instance, with debugs) CME gateway will experience the problem less often.

- CSCsq15994

  Symptoms: Low CPS may be observed.

  Conditions: The symptoms are seen with PPPoA and PPPoE sessions.

  Workaround: There is no workaround.

- CSCsq16611

  Symptoms: IPv6 packets are process switched instead of using Cisco Express Forwarding (CEF).

  Conditions: The above symptom is observed on a Cisco 7301 and Cisco 7200 routers.

  Workaround: There is no workaround.

- CSCsq18737

  Symptoms: A router may crash and tracebacks may be seen upon reconfiguring object-groups.

  Conditions: The symptoms are observed when the router is configured with an initial object-group configuration. If the object-group is reconfigured with two IP hosts, the router crashes.

  Workaround: There is no workaround.

- CSCsq19047

  Symptoms: A VXML gateway may stop handling calls due to lack of memory. The memory leak occurs in Chunk Manager process.

  Conditions: The symptom is observed on a VXML gateway that is running Cisco IOS Release 12.4(15)T and when the SIP Take back application is configured to initiate a REFER-based call transfer in a CVP scenario.

  Workaround: There is no workaround.

  Further Problem Description: Page 374 of the following configuration and administration guide states how this configuration must be set up:

  http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp4_0/configuration/guide/cvp40cfg.pdf

- CSCsq20970

  Symptoms: On the Cisco 2432 platform UUT, the “atm” option is missing in the “mode” CLI when the T1 controller is being configured for ATM.

  Conditions: The symptom is observed on the Cisco 2432 platform with a T1 controller.

  Workaround: There is no workaround.

- CSCsq21347

  Symptoms: Sometimes WebVPN login page may not come up when a client browser connects to the gateway. Sometimes, login page may come up, but after entering the login credentials portal page does not come up. The following syslog messages are seen.

  1) We are able to enter the webvpn login page, but after entering the username and password, the page returns the error message “Internal Error” and does not let us login. Also, the traceback below is seen.

  ```
  May 10 06:15:19.183 PDT: %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 0 for chunk
  0, data 0 -Process= "SSLVPN_PROCESS", ipl= 0, pid= 265, -Traceback= 0x61898E8C
  0x6002DFC4 0x63D802FC 0x63D70C64 0x63D78A5C 0x63D79054 0x63D7986C 0x63D736A8
  ```

  2) The webvpn login page is not thrown up at all when we try to connect to the webvpn gateway. The “Page is not displayed” due to the following traceback:

  ```
  May 10 21:57:30.963 PDT: %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type 0 for chunk
  0, data 0 -Process= "IP Input", ipl= 0, pid= 120, -Traceback= 0x61898E8C 0x6002DFC4
  0x63D6D564 0x63D72F48 0x63D5C804 0x62285B20 0x62288158 0x61F81940 0x61F83264
  0x61F8367C 0x61F83738 0x61F83980
  ```

  Conditions: This can happen if WebVPN configuration is being removed and a client tries to connect.

  Workaround: Avoid removing WebVPN configuration once it is configured.

- CSCsq24672

  Symptoms: A call through CUBE may not establish for a Re-Invite-based call flow. The call may drop.

  Conditions: This symptom is observed if the endpoint to which the CUBE is communicating sends a Re-INVITE for a call before it has received an ACK from the other call leg for the original INVITE. CUBE may not forward this Re-Invite to the other call leg, and the call will disconnect.

  Workaround: There is no workaround.

- CSCsq24935

  Symptoms: A switch reloads when the **distance bgp** command is configured under ipv6 address family.

  Conditions: This symptom is observed on a Cisco 3560 that is running Cisco IOS Release 12.2(44)SE2. The same symptom is also seen on a Cisco 3750. The following commands are issued:

  ```
  router bgp <>
   address-family ipv6 unicast
   distance bgp <> <>
  ```

  The router subsequently reloads because of an Instruction access Exception.

  Workaround: There is no workaround. BGP/ipv6 is not supported on such platforms.

- CSCsq26111

  Symptoms: The extension number and speed dial number may not be displayed in full-length on a fallback ephone.

  Conditions: The symptom is observed after an ephone falls back to the SRST.

  Workaround: There is no workaround.

- CSCsq29623

  Symptoms: A Cisco AS5350 or Cisco AS5350XM that is running Cisco IOS Release 12.4(15)T5 will drop incoming VPN traffic larger than 512 bytes when the traffic is destined for a dialer interface.

Conditions where problem is seen:

- When packets arrive on a crypto tunnel that terminates on the Cisco AS5350 AND when the packets are destined for a destination that is reachable over a dialer interface.
- With a legacy dialer-map or dialer-pool DDR configuration. No difference is seen between the two.
- With CEF disabled.

Conditions where problem is not seen:

- Without crypto.
- With process-switching (CEF and fast-switching disabled).
- When packets are destined for a host that is reachable via an Ethernet interface.

Workaround: There is no workaround.

- CSCsq30717

  Symptoms: A NPE-G1 resets due to a hardware watchdog timeout. This is indicated in the **show version** output with "Last reset from watchdog reset."

  Conditions: The Cisco 7200 must have an enabled PA-MC-2T3-EC with channelized T1s.

  Workaround: Disable the PA-MC-2T3-EC.

- CSCsq31592

  Symptoms: Applying service policy on output interface causes the router to crash.

  Conditions: Device crashing with "set_service_policy_checkpoint_bit" when output service-policy is applied on serial/ATM sub-interfaces.

  Workaround: There is no workaround.

- CSCsq31808

  Symptoms: With eiBGP multipath, incoming labeled packets may get looped in MPLS core instead of getting forwarded to CE, causing traffic issues. The following symptom may be found:

  - The error message below is frequently generated.

    ```
    Dec 17 07:44:46.734 UTC: %COMMON_FIB-3-BROKER_ENCODE: IPv4 broker failed to encode
    msg type 0 for slot(s) 0B -Traceback= 6044E470 60465864 6043BCFC 6043B570
    ```

  - The **debug cef xdr** command yields the following message:

    ```
    Mar 31 17:44:40.576 UTC: FIBrp_xdr: Table IPv4:<vrf name>, building insert event
    xdr for x.x.x.x/y. Sources: RIB Mar 31 17:44:40.576 UTC: FIBrp_xdr: Encoding path
    extensions ... Mar 31 17:44:40.576 UTC: FIBrp_xdr: - short ext, type 1, index 0
    Mar 31 17:44:40.580 UTC: FIBrp_xdr: Getting encode size for IPv4 table broker
    FIB_FIB xdr Mar 31 17:44:40.580 UTC: - short path ext: len 12 Mar 31 17:44:40.580
    UTC: - short path ext: len 24 Mar 31 17:44:40.580 UTC: - feat IPRM, len 12 Mar 31
    17:44:40.580 UTC: => pfx/path 113 + path_ext 24 + gsb 8 + fs 16 = 161
    ```

  - Checking the prefix, it points to drop entry.

    ```
    Router# show mpls forward vrf <vrf name> x.x.x.x

    Local Outgoing Prefix Bytes Label Outgoing Next Hop Label Label or VC or Tunnel Id
    Switched interface 937 No Label x.x.x.x/y[V]  0 drop <========= it is drop
    ```

  - Checking the MOI flag of EBGP path, the No_Global flag (0x10) was incorrectly set.

    ```
    Router# show ip cef vrf <vrf name> x.x.x.x int

    [snip]
    path_list contains at least one resolved destination(s). HW not notified path
    70BFFC5C, path list 20E87B58, share 1/1, type recursive nexthop, for IPv4, flags
    resolved MPLS short path extensions: MOI flags = 0x16 <-------MOI flags 0x10 is
    ```

```
incorrectly set (for ebgp path, correct flag should be 0x4, 0x5, 0x6 ..) correct
now.
[snip]
```

Conditions: The eiBGP multipath is enabled; iBGP path comes up first and then the eBGP path. Both eBGP and iBGP paths could be in MPLS forwarding causing the issue.

Workaround: Use the **clear ip route vrf <name> x.x.x.x** command to clear the issue.

- CSCsq31958

  Symptoms: In a network with redundant topology, an Open Shortest Path First (OSPF) external route may remain stuck in the routing table after a link flap.

  Conditions: Problem observed in Cisco IOS Release 12.4T. Not present in Cisco IOS Release 12.3T.

  Workaround: The issue can be resolved by entering the **clear ip route** command for the affected route.

- CSCsq33653

  Symptoms: The caller ID transmission may fail from FXS port to FXO port.

  Conditions: The symptoms are observed when the sub-command **caller- id** is configured under "voice-port x/y."

  Workaround: There is no workaround.

- CSCsq34171

  Symptoms: A router may crash when the ip address/mask is changed on the interface.

  Conditions: The symptom occurs if EIGRP authentication is enabled.

  Workaround: Disable authentication.

  Further Problem Description: When the authentication is removed from the interface, the crash does not occur on changing the mask.

- CSCsq35036

  Symptom: An HWIC-1DSU-T1 card comes up with line loopback turned on.

  Conditions: The symptom is observed with Cisco 2801 and 1841 routers only.

  Workaround: Press the pushbutton to clear loopback condition.

  Alternate workaround: Execute the **clear service-module <>** command.

  Further Problem Description: The problem happens because HWIC reset assert/deassert is not happening before and after the FPGA download respectively in these platforms.

- CSCsq37010

  Symptoms: Unable to set up SSL VPN full-tunnel from clients.

  Conditions: Occurs on Cisco 3845 router running the c3845-adventerprisek9-mz.124-19.18.T2 image. When Windows client attempts to connect, tunnel set up fails with error "The VPN client driver has encountered an error."

  Workaround: There is no workaround.

- CSCsq37349

  Symptoms: A router may crash due to a corrupted Program Counter.

  Conditions: The symptom is seen with Zone-based Firewall and IPS, along with VRF and IPSec tunnel configured.

  Workaround: There is no workaround.

- CSCsq39244

  Symptoms: IPv6 traffic going to a 6PE device may be dropped after an interface flap.

  Conditions: The symptom is observed when the IPv6 prefix is known by BGP and the same prefix is assigned to the local interface. After an interface flap, the MPLS forwarded table is populated with drop and all incoming 6PE traffic going to that interface is dropped.

  Workaround: There is no workaround.

- CSCsq40088

  Symptoms: A Cisco 3845 router may crash when unconfiguring IPv6 nodes.

  Condition: The symptom is observed on a Cisco 3845 router that is running Cisco IOS Release 12.4T. The traceback is produced after configuring the **no ipv6 unicast-routing** command.

  Workaround: There is no workaround.

- CSCsq40649

  Symptoms: Card is crashing while entries are being added to the access list.

  Condition: Occurs when additional entries are being added to an access list that is already attached to an interface. The card is crashing with memory corruption.

  Workaround: There is no workaround.

- CSCsq40659

  Symptoms: A client may not get a prefix when it has two relay agents on two interfaces of a single DHCP relay agent, with one of them being an unnumbered interface.

  Conditions: The symptom is seen on a router that is running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsq40813

  Symptoms: Queue-limit locked with the given value and remains dead with “random-detect discard-class-based.”

  Conditions: Happens only with random-detect discard-class-based and queue-limit configuration.

  Workaround: There is no workaround.

- CSCsq41455

  Symptoms: The router hangs and has to be reset.

  Conditions: This crash happens when out-of-order sequence numbers are used in an ACL. In the ACL in the description, ACE 1 triggers the crash.

  Workaround: Instead of making the changes to the ACL with the ACL applied to the interface, if the changes are made to the ACL after it is removed from the interface, the crash will not happen.

- CSCsq41508

  Symptoms: An ACL with more than 13 ACEs will not show any matches on the OG ACEs.

  Conditions: If the ACL has more than 13 ACEs, any object group ACEs will not function properly.

  Workaround: There is no workaround.

- CSCsq42399

  Symptoms: Shortly after upgrade, the router shows the following error:

  ```
  May 22 09:05:53.109 METDST: %SYS-2-MALLOCFAIL: Memory allocation of 261116 bytes
  failed from 0x61A37948, alignment 0 Pool: Processor Free: 6427012 Cause: Memory
  fragmentation Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "Virtual
  ```

```
Exec", ipl= 0, pid= 234, -Traceback= 0x61452110 0x6000A7FC 0x60010638 0x60010C2C
0x634CB644 0x61A37950 0x61461910 0x 614BD940 0x6149E000 0x614C1B08 0x62AA2494
0x62AA2478
```

Traffic is affected, and the router is unable to display output from the **show run** command.

Conditions: Occurs on a Cisco 7200 router running the c7200-adventerprisek9-mz.124-15.T3.bin. Service Selection Gateway (SSG) and RADIUS are involved.

Workaround: There is no workaround.

- CSCsq43591

  Symptoms: When a session is cleared from the CPE and when it reconnects instantaneously, a ping fails to the CPE.

  Conditions: This symptom is observed under the following conditions:

  - LAC<->LNS setup.
  - Clearing of session from CPE.
  - In the **show pxf cpu vcci** command output, there is no VCCI present for the VAI.
  - Also seen in lab when the CPE is booted and the first session comes up.

  Workaround: Clear the VAI interface from the LNS. The session will reconnect and will work fine.

- CSCsq43831

  Symptoms: A Cisco IOS router may unexpectedly reload when Forwarding Information Base (FIB) processes an adjacency for route that has many levels of recursion.

  Conditions: This has been seen only after the following error message was displayed:

  ```
  %COMMON_FIB-6-FIB_RECURSION: 10.10.10.1/32 has too many (8) levels of recursion during
  setting up switching info
  ```

  Workaround: Change static routes so they specify both the interface and next-hop instead of just specifying the next-hop. For example change

  ```
  ip route 10.0.0.0 255.255.255.255 192.168.1.1
  ```

  to

  ```
  ip route 10.0.0.0 255.255.255.255 GigabitEthernet1/0 192.168.1.1
  ```

  This is particularly true when using eBGP between loopbacks to allow for multiple parallel links between the two eBGP peers, where one typically installs static routes for the eBGP peers address. Make sure these static routes have both interface and next-hop specified.

- CSCsq43934

  Symptoms: TCP/HTTP zone-based firewall (ZBF) session failed to established with dynamic or overload NAT mode.

  Conditions: Normal deployment condition.

  Workaround: There is no workaround.

- CSCsq44428

  Symptoms: Under certain conditions with IPv6 for EIGRP, the router may log error messages such as the following:

  ```
  00:00:09: %DUAL-3-INTERNAL: IPv6-EIGRP(0) 80: Internal Error
  ```

  Conditions: The error message is currently not causing a operational impact.

  Workaround: There is no workaround.

- CSCsq44598

  Symptoms: A PA-POS-2OC3 experiences an output stuck condition.

Conditions: This issue is sporadic in nature and is sometimes seen with QoS configurations although QoS is not the cause of the issue. The issue is due to an extra interrupt, which is confusing the driver if it expires before the FIFO reaches the low point. For example, if the FIFO goes full but is filled with large packets, then it is possible that the no traffic timer will expire before the tx packets have emptied. It is a communication issue between the hardware and the driver code.

Workaround: There is no workaround.

- CSCsq45836

  Symptoms: Dynamic Multipoint VPN (DMVPN) shortcut tunnels may fail to get established on a DMVPN spoke running a phase 3 setup.

  Conditions: Occurs in Cisco IOS Release 12.4(20)T.

  Workaround: There is no workaround. However, data traffic would not be affected since the packets would take the spoke-hub-spoke path.

- CSCsq46742

  Symptoms: SIP gateway crashes when a 302 response contains a contact header with the same IP address as that of SIP gateway.

  Conditions: The crash occurs only when the 302 response contains a contact header with an IP address the same as that of the gateway IP address. The crash also occurs only when the IP address is mapped to a domain name exceeding the length of the IP address received in the contact header.

  Workaround: Ensure that the IP address that is received in the 302 response is mapped to a domain name not exceeding the length of the IP address.

- CSCsq46832

  Symptoms: The “IP SLAs: RTP VoIP Operation” feature was introduced in Cisco IOS Release 12.4(4)T to allow users to obtain some realistic VoIP Round Trip Time (RTT), Jitter, Packet Loss, and Mean Opinion Score (MOS) measurements from a live VoIP call over a real IP cloud and using a bonafide voice codec supported over voice DSPs. It has been found that in certain versions of the Cisco IOS 12.4T release train, this feature is not functioning at all. The output of the **show ip sla statistics N** EXEC command, where N is the IP SLA probe tag number, returns something similar to the following output reporting all zeroed-out measurements:

  ```
  VoiceGateWay# show ip sla statistics 3 IPSLAs Latest Operation Statistics

  IPSLA operation id: 3 Type of operation: rtp Latest operation start time: 11:35:15.606
  EST Tue May 27 2008 Latest operation return code: No connection Latest RTT
  (milliseconds): 0 Source to Destination Path Measurements: Interarrival Jitter: 0
  Packets Sent: 0 Packets Lost: 0 Estimated R-factor: 0 MOS-CQ: 0.00 Destination to
  Source Path Measurements: Interarrival Jitter: 0 Packets Sent: 0 Packets Lost: 0
  Estimated R-factor: 0 MOS-CQ: 0.00 Operation time to live: 72083 sec Operational state
  of entry: Active Last time this entry was reset: Never
  ```

  Conditions: This behavior is observed on Cisco 1700, 2600, 3700, 7200, 7500, 2800, and 3800 voice platforms installed with Cisco IOS Release 12.4(19.18)T or later releases and configured with the RTP VoIP IP SLA feature.

  Workaround: There is no workaround.

- CSCsq48201

  Symptoms: A crash may occur when creating a Bridge-Group Virtual Interface (BVI) while traffic is flowing.

Conditions: The crash could occur when a BVI interface is first created with the command **interface BVI** and traffic is being process switched by a physical interface in the same bridge-group. Once the BVI interface is created, subsequent **interface BVI** commands to configure that interface will not cause the crash.

Workaround: Remove the physical interface from the bridge-group, or prevent traffic from being process switch by the interface when the BVI interface is first created.

- CSCsq48717

  Symptoms: Attaching the following policy:

  ```
  policy-map p1
   class prec1
   class class-default
    shape
  ```

  Will result in the packets to class prec1 not being enqueued to class-default.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(19.18)T02.

  Workaround: Remove the policy from the interface, remove class prec1, add the policy back and then add class prec1.

- CSCsq48949

  Symptoms: A hierarchical policy cannot be attached.

  Conditions: This symptom is observed with a Cisco 7200 router that is running Cisco IOS Release 12.4(19.18)T2.

  Workaround: There is no workaround.

- CSCsq49100

  Symptoms: Removal of last class-map before the qos-group class-map causes the router to crash.

  Conditions: Happens every time when the class-maps change from type(Mix) to type(Un-Mix), such as the following:

  Mix: dscp precedence qos-group

  Un-Mix: qos-group qos-group qos-group

  Workaround: There is no workaround.

- CSCsq49768

  Symptoms: MAC L2TP clients failed to setup tunnel after L2TP network server (LNS) upgraded to Cisco IOS Release 12.4(19.18)T3.

  Conditions: Occurs when Mac OS X 10.4 and Mac OS X 10.5 clients attempt to connect to a LNS running Cisco IOS Release 12.4(19.18)T3. image loaded.

  Workaround: There is no workaround.

- CSCsq49816

  Symptoms: Adding a service policy to a PVC under switch subinterface with PPP multilink configured will cause PXF queue size to become misprogrammed.

  Conditions: Occurs when policy-map with priority class is attached to a MLP PVC under switch sub-interface and the MLP bundle is down. The PXF switch1 queue will be misprogrammed.

  Workaround: Such a configuration is not allowed and has to be avoided.

- CSCsq50047

  Symptoms: A router may crash when a service policy is applied to a Frame Relay map-class.

Conditions: This symptom is observed when the minimum committed information rate (minCIR) is lowered, causing an already attached policy to no longer have enough bandwidth. Then the service policy is removed, and when it is reconfigured, the crash occurs.

Workaround: There is no workaround.

- CSCsq50100

  Symptoms: When a call is placed between secure phone from SIP gateway to secure Cisco Unified CallManager (CCM) phone call is established as SRTP call. After hold/resume the call becomes non-secure.

  Conditions: All supplementary services are affected (hold/resume of a secure call, call transfer, conferencing, etc.).

  Workaround: There is no workaround.

- CSCsq51119

  Symptoms: A Cisco router may unexpectedly reload because of a bus error.

  Conditions: The router must be running NHRP and be having the NHRP SNMP MIB polled.

  Workaround: Stop polling the NHRP SNMP MIB.

- CSCsq51500

  Symptoms: When attempting to bring up the Secure Device Provisioning (SDP) Welcome page, the following message is displayed in the web browser: “IPv6 unicast-routing is not enable”.

  When using Internet Explorer, this is simply a cosmetic bug. With Firefox v2.0.0.14, this message gets displayed and the web page is corrupted and unusable so that SDP cannot continue.

  Conditions: When the config is saved and you do not have IPv6 unicast routing enabled, this problem sometimes occurs when attempting to display the SDP Welcome page.

  Workaround: Use Internet Explorer rather than Firefox.

- CSCsq51517

  Symptoms: QOS classification post-encryption is not working.

  Conditions: The symptoms are observed when using QoS post-classification (classification after encryption) of packets.

  Workaround: There is no workaround.

  Further Problem Description: With the changes introduced in CSCsq07294, Cisco IOS Release 12.4(20)T will no longer support QoS classification post-encryption.

- CSCsq51826

  Symptoms: Router crashes when Flexible NetFlow for IPv6 is received and IPv6 fragmented packets are received.

  Conditions: Flexible NetFlow for IPv6 must be configured, and fragmented IPv6 packets must be received.

  Workaround: Deconfigure IPv6 Flexible NetFlow.

- CSCsq52048

  Symptoms: Router crashed while running **show vpdn tunnel all** command.

  Conditions: When there are thousands of L2TP tunnels coming up, going down, running the **show vpdn tunnel all** command may result in crash.

  Workaround: There is no workaround.

- CSCsq52847

  Symptoms: Connection establishment failed with the event agent.

  Conditions: Occurs when the Event Gateway is killed and restarted on a Cisco 1812 router while running Cisco IOS Release 12.4(19.18)T2.

  Workaround: There is no workaround.

- CSCsq54601

  Symptoms: SCCP and SIP registration fail with EzVPN and NAT configured. Only Voice traffic is affected.

  Condition: Occurs when SCCP Registration traffic is passing through NAT router.

  Workaround: There is no workaround.

- CSCsq56103

  Symptoms: Configuration issues occur on serial interfaces.

  Conditions: Two different issues occur:

  – When a strict policy is applied on a serial interface, if the user re-configures the strict priority configuration under the same class in the same policy, it will fail.

  – When the user tries to remove the service policy from the serial interface, The HQF data structure is not cleaned up. The class default BLT and physical interface BLT are not deleted.

  Workaround: There is no workaround.

- CSCsq57856

  Symptoms: When Cisco 2431 and Cisco 2691 router is configured with 1DSU-T1-V2 card, router crashes while loading.

  Conditions: The crash is seen while loading the router, when router is configured with 1DSU-T1-V2.

  Workaround: There is no workaround.

- CSCsq58748

  Symptoms: When a OCSP (Online Certificate Status Protocol) request is made for checking the revocation status for a certificate to the OCSP server, if under some circumstances the TCP connection for the OCSP request goes into a stalled state, then the IKMP process can get blocked. This can cause the router to be unable to process any further IKE packets, and can stop any new tunnel negotiations/rekeys/DPDs from occurring. Existing IPSEC SAs will continue to work until a rekey or DPD is triggered.

  Condition: Occurs on a Cisco IOS router with IPSec VPN and certificates and configured for revocation checking.

  Workaround: Perform the following steps:

  1) Disable revocation checking and then reload.

  2) Reload the router.

- CSCsq60016

  Symptoms: A router crashes after a long RSA key string is entered.

  Conditions: This symptom is observed when a very long hex string is entered.

  Workaround: Break the entry into shorter strings.

- CSCsq60750

  Symptoms: The “Net Input” process can cause Cisco 2800 and Cisco 2811 routers to crash.

Conditions: Occurs on the Cisco 2800 and Cisco 2811 routers when loaded with Cisco IOS Release 12.4(19.18)T2.

Workaround: There is no workaround.

- CSCsq60952

  Symptoms: Traffic is mis-classified when it arrives on a sub-interface and firewall is configured on the tunnel interface.

  Conditions: Occurs on routers running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsq61398

  Symptoms: L2TP/IPSec connections fail between Cisco 1800 clients and the Cisco 7200 server when the server is configured for hardware encryption.

  Conditions: Occurs with the following topology:

  User---1811 (LAC) F0/0 ------- Router--ASA---G0/1 c7200 (LNS)

  Occurs when Cisco 1800 routers are L2TP-over-IPsec clients, terminating their connection to a Cisco 7200. The problem exists in Cisco IOS Release 12.4(15)T3 and Cisco IOS Release 12.4(15)T4.

  Workarounds: Disable fast switching/CEF on the Cisco 7200. By entering the **no ip route-cache** command under both interface gigx/y and virtual-template xx of the Cisco 7200, the L2TP connection is stable.

```
int Gig Ethernet X/Y
 no ip route-cache
int virtual-template XX
 no ip route-cache
```

- CSCsq62269

  Symptoms: If a Cisco 3270 has no startup configuration, it will crash if the “autoinstall” option is selected.

  Condition: Occurs when there is no startup configuration and the router is using the c3270-adventerprisek9-mz.124-15.XZ.bin image.

  Workaround: Execute **tftpdnld -r in rommon to boot c3270-entbase-mz.124-15.XZ.bin**. Do not allow the “autoinstall” option to run. Save the default configuration and reboot it with the c3270-adventerprisek9-mz.124-15.XZ.bin image.

- CSCsq63176

  Symptoms: PA-MC-T3/E3-EC PA does not pass full traffic after a sudden burst near line rate.

  Conditions: Occurs when 256 interfaces are configured on the port adapter with multilinks operating on those serial interfaces.

  Workaround: Configure fewer than 256 serial interfaces.

- CSCsq63278

  Symptoms: Shape rate under child policy is not met. Shape rate of child policy is equal to parent shape rate

  Conditions: Occurs on a Cisco 7200 router is running Cisco IOS Release 12.4(21.1)T.

  Workaround: There is no workaround.

- CSCsq63731

  Symptoms: If either the command **vlan-id dot1aq** *vlan-id* or the command **vlan-range dot1aq** *start-vlan-id end-vlan-id* is configured on a main interface which is also configured for routing, and an ARP packet is sent to the router on the configured VLAN, then the router may send an ARP reply with a VLAN ID of zero.

  Conditions: The symptoms are seen on a Cisco 2800 series and a Cisco 7200 series router when the command **vlan-dot1q** *vlan-id* is configured on the GigabitEthernet interface of a Cisco 2800 series router and **encapsulation dot1q** *vlan- id* is configured on the FastEthernet 2/1/2.1 interface.

  Workaround: Change the Cisco 2800 series router's (CE) configuration to use a sub-interface for the vlan-id instead of using the **vlan- dot1q** *vlan-id* command on the main interface. With a sub-interface configured on the 2800, we can verify that the ARP packets are sent with proper VLAN ID.

- CSCsq64663

  Symptoms: Router Crashes when EtherChannel is shut down

  Conditions: Occurs on a Metro Ethernet device with over 2000 IP SLA operations configured and CFM services defined for a EtherChannel. The **no int ether-channel ...** command causes the device to crash.

  Workaround: There is no workaround.

- CSCsq64843

  Symptoms: An IOS router configured with Dynamic Multipoint VPN (DMVPN) may run of memory.

  Conditions: The symptom may occur when hub or spoke is behind a NAT device.

  Workaround: There is no workaround.

- CSCsq67163

  Symptoms: Scheduling of IP SLA RTP operation crashes the router.

  Conditions: This problem occurs only when IPSLA RTP operation is configured and scheduled to run.

  Workaround: There is no workaround.

- CSCsq70248

  This caveat fixes the wrong code (cc_patch issue) committed by CSCsm74168. See CSCsm74168 below.

  CSCsm74168

  Symptoms: Cisco Unified Border Element (CUBE) crashes when operating in SIP to SIP mode. This will happen if CUBE has received REFER on one leg and tries to send INVITE on the other leg as a part of a call-transfer.

  Conditions: Topology:

  [CRASH] Org.--(SIP Trk)--CSPS--(SIP Trk)--CUBE1--(SIP Trk)--CUBE2--(H323 Trk)--Term_1 | | (H323 Trk) | Term_2

  Call is established between Org. and Term_1 and the originator attempts to transfer the original call to a second party on the Term_2 side. When Term_2 answers, CUBE1 crashes.

  Workaround: There is no workaround.

  Further Problem Description:

CUBE1 in detail: X-OR----------CUBE1--------(Term_1)X-EE----- | | | CUBE2 | | -----(Term_2)X-TO----------

X-EE and X-OR operate in SIP-SIP mode. When it tries to set up a new call to Term_2, it tries to get channels, xcaps, callParams info from the peer leg (the Term_1 leg is the peer leg for Term2). The Term_1 call leg passes channels, xcaps, but does not pass callParams details (that contains the operating mode). So the Term_2 leg takes the default and sets its mode as SIP- H323 and executes some of the H323 related function. The result is undefined and this leads to the crash.

- CSCsq70473

  Symptoms: An MWAM processor Gigabit Ethernet interface stops processing traffic.

  Conditions: This symptom is observed at a high rate of incoming traffic.

  Workaround: Restart the interface (enter the **shutdown** command followed by the **no shutdown** command) to restore traffic forwarding.

- CSCsq70588

  Symptoms: A router's memory may become corrupted, which can lead to a crash.

  Conditions: This symptom is observed when Flexible NetFlow is configured with a record that has a large packet section in it, and it is applied to capture traffic.

  Workaround: Configure Flexible NetFlow with a flow record that does not have a packet section in it.

- CSCsq70872

  Symptoms: Router crashes when executing the **clear zone-pair inspect session** command.

  Conditions: Occurs when the router has a TCP session active when the user executes the command.

  Workaround: There is no workaround.

- CSCsq71095

  Symptoms: SSL connection over L2TP IPSec tunnel does not work. Checksum errors on the Change Cipher Spec messages coming from the server.

  Conditions: This has been seen on a Cisco 7200 running Cisco IOS Release 12.4(15)T5 and the ADVENTERPRISEK9-M image. A Cisco 2821 with the same version and feature set was not affected.

  Workaround: Use a router other than the Cisco 7200 for this task, or disable IPSec and only use SSL over L2TP.

- CSCsq71492

  Symptoms: A Cisco IOS device may reload with an address error or have alignment errors and tracebacks such as %ALIGN-3-SPURIOUS or %ALIGN-3-TRACE.

  Conditions: The symptoms are most likely to occur when the TACACS+ server (ACS) sends an "authentication error" when ACS is configured, or when a request timeout occurs. There may be other AAA or TACACS related conditions that cause the symptom.

  Workaround: There is no workaround.

- CSCsq74300

  Symptoms: Loopbacks, Null0, and other non-Point-to-Point interfaces are not allowed in a **route-map set** command because of the changes introduced with caveat CSCsk63775.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(18) or a later release. Upgrading to Cisco IOS Release 12.4(18) or a later release may break the existing network.

  Workaround: Use Cisco IOS Release 12.4(17) or an earlier release.

- CSCsq74307

  Symptoms: The PfR MC may reload.

  Conditions: This symptom is observed if the PfR BGP inbound feature is enabled, and inbound prefixes are configured and controlled by PfR, and the **clear ip bgp *** command is executed on the controlling BR.

  Workaround: Do not configure inside prefixes; instead, let PfR learn using the following configuration:

  ```
  oer master
   learn
    inside bgp
  ```

- CSCsq75526

  Symptoms: When DNS forwarding source interface is configured in a split DNS environment, the source address being populated in the packet while forwarding the DNS query is wrong. It always takes the first interface in the VPN routing/forwarding (VRF) view even when the DNS forwarding source interface is changed. DNS query fails.

  Conditions: The above symptom is seen on a router running Cisco IOS Release 12.4(15)T6.

  Workaround: There is no workaround.

- CSCsq75944

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly. On the console or in the RP crashinfo file, the following message can sometimes be seen:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.
  ```

  Conditions: Occurs during normal use on a Catalyst 6500 or Cisco 7600. NetFlow must be enabled.

  Workaround: Disable NetFlow by using one of the following commands on every sub-interface for which NetFlow is configured:

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

- CSCsq76338

  Symptoms: Call across SIP trunk takes around 10 seconds to resume after called party goes on hold.

  Conditions: Occurs during normal operating conditions.

  Workaround: There is no workaround.

- CSCsq77968

  Symptoms: Changing the connect command configuration may reload the router.

  Conditions: Occurs when the same connection is configured twice with different interfaces and Data-Link Connection Identifiers (DLCI). This is observed when running the latest version of Cisco IOS Release 12.4T.

  Workaround: Instead of changing the connect command configuration, use the **no connect** command to remove the command and then re-apply the new connect command configuration.

- CSCsq78208

  Symptoms: The router is crashing during start up when NTP update is received from SUP.

  Conditions: Occurs when there is an NTP update and a Cisco Multi-Processor WAN Application Module (MWAM) is present.

  Workaround: There is no workaround.

- CSCsq80546

  Symptoms: Router crashed when policy-map modified while passing traffic.

  Conditions: The problem was seen on Cisco routers running Cisco IOS Release 12.4(19.18T5).

  Workaround: There is no workaround.

- CSCsq80658

  Symptoms: H325 call is not connected properly in Cisco Unified Border Element (CUBE).

  Conditions: In CUBE, tokens received in H225 CONNECT will be not passed to the other leg if the following CLI is enabled:

  voice service voip supplementary-service media-renegotiate

  Workaround: Disable the **supplementary-service media-renegotiate** command under **voice service voip**.

- CSCsq81073

  Symptoms: MGX RPM-XF backcard is reset when the **test rpm ecc 1bit** command is entered.

  Condition: Occurs on an MGX with two-port gigabit Ethernet and two-port POS backcards.

  Workaround: There is no workaround.

- CSCsq81116

  Symptoms: Router may reload when Optimized Edge Routing (OER) master configuration is **shut/no shut**.

  Conditions: Only occurs when OER master controller goes down and then rarely.

  Workaround: There is no workaround.

- CSCsq81235

  Symptoms: A VRF cannot be configured again when it is deleted by using the **no ip vrf** command.

  Conditions: This symptom is seen only on VRFs with an MDT tunnel.

  Workaround: There is no workaround.

- CSCsq83872

  Symptoms: There may be a memory leak when the **no pppoe enable** command is applied.

  Conditions: This symptom is observed on a Cisco 831 router.

  Workaround: There is no workaround.

- CSCsq85615

  Symptoms: Phones stay registered to Cisco Survivable Remote Site Telephony (SRST) router and do not re-register to Cisco Unified CallManager (CCM) after connectivity is restored.

  Conditions: This problem affects only phones that use SIP/UDP for signaling. SIP/TCP and SCCP phones are not affected.

  Workaround: Reloading the phones will resolve this issue (temporarily, until the next loss of connectivity). To avoid the problem, do not configure IOS firewall on any router between a SIP/UDP phone configured for SRST and the CUCM.

  Further Problem Description: The problem is caused by IOS FW blocking the packets from the CCM that would notify the phone that the CCM is accessible.

- CSCsq86067

  Symptoms: Router will crash while configuring match access-group name with longer string.

Conditions: Occurs when match access-group name is configured with string length greater than 122 characters.

Workaround: There is no workaround.

- CSCsq89122

  Symptoms: Cisco 7206VXR with NPE-G1, SA-VAM2+, and PA-A3-OC3MM may generate spurious memory accesses.

  Conditions: One possible trigger may be ATM link instability.

  Workaround: There is no workaround.

- CSCsq90567

  Symptoms: The TSP gets stuck in connected state.

  Conditions: Occurs after resuming an onhold shared DN from the associated ephone. The TAPI gets stuck.

  Workaround: There is no workaround except rebooting the ephone and the TAPI.

- CSCsq91342

  Symptoms: CUBE will truncate the Calling Number IE when passing through an MWI SETUP.

  Conditions: This symptom is observed in Cisco IOS Release 12.4T. Cisco IOS Release 12.3T works fine.

  Workaround: There is no workaround.

- CSCsq91960

  Symptoms: VRF may not get deleted if the VRF NAME size is 32 characters on a dual RP HA/SSO router.

  Conditions: This symptom occurs when adding a VRF with 32 characters on a DUAL RP HA router. (In some releases a VRF name with more than 32 characters will get truncated to 32.) The following may occur:

  - There may be a DATA CORRUPTION ERRMSG.
  - While deleting this 32 character length VRF, VRF will fail to get deleted completely with an ERRMSG on active.

  Workaround: There is no workaround.

- CSCsq92063

  Symptoms: Router may crash.

  Conditions: This symptom is observed when Flexible NetFlow is configured with a flow record that includes layer 4 fields and the flow monitor is applied to IPv6 traffic, and the traffic that FNF is monitoring has a payload length that does not allow us to reach the transport header in the IPv6 packet.

  Workaround: Configure Flexible NetFlow with a record that does not have any layer 4 (transport) fields.

- CSCsq93564

  Symptoms: When Cisco 7965 and Cisco 7975 IP phones with add-on modules (7914/7915/7916) fall back to Cisco Survivable Remote Site Telephony (SRST), only 6 to 8 lines are available during SRST fallback.

  Conditions: This problem occurs when phones are registered on Cisco Unified CallManager (CCM) 6.1 fallback to SRST 4.3.

Workaround: There is no workaround.

- CSCsq94036

  Symptoms: Packets are hardware-switched after applying IP precedence. The expected behavior here is that packets are software-processed when “ip precedence” is applied over “ip next-hop” because applying a policy over the other wipes the adjacencies that were already established.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SX or 12.2SR.

  Workaround: There is no workaround.

- CSCsq94677

  Symptoms: The second channel for a dual-line DN or the eighth channel for octo-line DN is not available for a fallback phone.

  Conditions: This problem occurs when a phone falls back to the Cisco Survivable Remote Site Telephony (SRST) the second time after the SRST reboots.

  Workaround: There is no workaround.

- CSCsr00711

  Symptoms: Cisco Unified Personal Communicator (CUPC) does not register with the server.

  Conditions: Occurs when Cisco IOS firewall is enabled on a router between the CUPC and the Cisco Unified Presence server. The CUPC is not able to register to the CUP server and consequently to Cisco Unified CallManager (CCM) either.

  Workaround: To avoid the problem, do not configure Cisco IOS firewall on any router between the CUPC and the CUP server.

- CSCsr00967

  Symptoms: A router crashes.

  Conditions: Clicking an application Citrix Server, for example a calculator, and, within a short period of time, clicking another application causes the router to crash.

  Workaround: There is no workaround.

  Further Problem Description: The router is crashing when a Citrix application is clicked and before it is launched another application is clicked. For the first application, the Cisco IOS gateway is waiting for a DNS resolution, and meanwhile TCP is closed, which is causing the appl_out_buffer of the corresponding context to be freed. Later, when the DNS resolution has come through, some data is attempted to be written to the server-side appl_out_buffer, and because it is null, the router is crashing.

  ```
  buffer==NULL check was missed in the function sslvpn_http_write_start_chunk before
  filling some data into it.
  Buffer NULL check is added in sslvpn_http_write_start_chunk function before accessing
  the buffer.
  ```

- CSCsr02593

  Symptoms: Incoming call incorrectly rings Skinny Call Control Protocol (SCCP) overlay.

  Conditions: An incoming call for DN 2 rings both SCCP phone A, which has the DN and another SCCP phone B without it but has an overlay line. DN 2 and overlay line aren’t shared line. Incoming call for the overlay only rings the overlay but incoming call for DN 2 will ring both.

  Workaround: Remove the overlay button from phone B, restart it, make an incoming to DN 2, add the overlay button back, restart phone. However, the problem will happen again after reload.

- CSCsr02848

  Symptoms: QoS policy is not getting attached to PPPATM session through virtual template.

  Conditions: This symptom is observed in a Cisco IOS Release 12.4(20)T image.

  Workaround: There is no workaround.

- CSCsr03713

  Symptoms: Secure Real-Time Transfer protocol (SRTP) calls failing.

  Conditions: Occurs with the following topology:

  OGW---SRTP,SIP-----TGW

  When SRTP is disabled, calls are passed.

  Workaround: Fall back to RTP.

- CSCsr06282

  Symptoms: A router reloads following an SNMP get operation.

  Conditions: Only occurs when a DHCP operation is configured with option-82 parameters.

  Workaround: Do not query MIB objects relating to the DHCP operation configured with option-82

- CSCsr08750

  Symptoms: A router may crash.

  Conditions: The router will crash with IO memory corruption when the **memory reserve critical** [**1-5**] command is executed.

  Workaround: Configure the **memory reserve critical** command with a much greater size.

  Further Problem Description: This issue occurs only when the ratio of free processor memory and free IO memory is high (say greater than 90).

- CSCsr09062

  Symptoms: Cisco 7200 crashes due to memory corruption.

  Conditions: Occurs when MLP+QoS is configured on a Cisco 7200 router. QoS policy is having bandwidth, change the BW parameter and flap the multilink using **clear int multilink1** to see the crash.

  Workaround: There is no workaround.

- CSCsr09400

  Symptoms: The packets decrypted with VSA hardware encryption and with CEF enabled while using L2TP protected by IPsec are not switched correctly.

  Conditions:

  1. Using the router as an L2TP termination hub.

  2. Using hardware encryption, specifically the VSA hardware engine.

  3. Using CEF switching.

  Workaround: There are several possible workarounds:

  - Disable CEF.
  - Apply the crypto map on the corresponding virtual-template interface alongside the physical interface.
  - Remove and reapply the crypto map (works until the next reboot).

  - Configure the **no ip route-cache** command and then the **ip route-cache cef** command on the virtual-template interface.

Further Problem Description: If this issue is reproduced in lab conditions, and the **debug ip packet detail** command is enabled, the following can be seen in the debugs:

```
*Jul 1 04:43:49.183: CEF: Try to CEF switch 10.175.135.48 from Virtual- Access2
```

The address in this message is “bogus” and corresponds to the data within the packet before the decryption, which essentially contains random bytes, so it can be anything.

- CSCsr10335

  Symptoms: A router loses its default gateway during autoinstall.

  Conditions: This issue was seen on Cisco IOS Release 12.4(15)T5, but should affect every Cisco IOS version.

  Workaround:

  1. Manually do a **shut** followed by a **no shut** on the interface.

  2. Create an EEM script, for example:

```
event manager applet Check-Default-Route event syslog pattern
"CNS-3-TRANSPORT: CNS_HTTP_CONNECTION_FAILED"
 action 1.0 cli command enable
 action 1.1 cli command config term
 action 1.2 cli command interface GigabitEthernet0/0
 action 1.3 cli command shut
 action 1.4 cli command no shut
 action 1.5 cli command end action 1.6 cli command write
!
 end
```

  3. In network-config, configure “ip address dhcp” for the interface that is supposed to get the default gateway from DHCP.

```
interface interface-name
ip address dhcp
end
```

- CSCsr11449

  Symptoms: The ingress decrypted packets do not get through with L2TP/IPSEC, even though they show up in the “decrypted” counter of the **show crypto ipsec sa** command output.

  Conditions: This symptom is observed when the **set nat demux** command is configured under the crypto map entry and when L2TP over IPSEC termination is used. VSA is used as the crypto engine.

  Workaround: There is no workaround.

- CSCsr12476

  Symptoms: Incrementing output queue drops on mGRE tunnel interface.

  Conditions: This symptom is observed on a Cisco 7206 NPE-G2 router that is running Cisco IOS Release 12.4(15)T6. This same symptom is not observed on a Cisco 7206-NPE-G1 that is running the same code.

  Workaround: There is no workaround.

- CSCsr14879

  Symptoms: The device crashes when it boots up.

  Conditions: Occurs on a router running the svcmwam-g8is-mz image.

Workaround: There is no workaround.

- CSCsr15478

  Symptoms: An input wedge is observed on an interface, when multicast traffic is flowing.

  Conditions: The symptom is observed in a DMVPN hub-spoke scenario with a point-to-multipoint (P2MP) GRE tunnel having tunnel protection configuration. When multicast traffic flows from hub to spoke through these tunnel interfaces, the incoming interface of the hub is getting wedged and even the ping to peer stops working.

  Workaround: There is no workaround, other than reloading the router.

- CSCsr16693

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

  Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

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

- CSCsr17429

  Symptoms: The build breaks after the commit of CSCsk39308, which brings IP CEF related enhancement into dialer.

  Conditions: The basic images do not include IP CEF subsystems. Hence, when we try to build them, the references to IP functions are not resolved.

  Workaround: There is no workaround.

- CSCsr18200

  Symptoms: A busy tone is not heard when a 183 message is received before a 4xx busy message.

  Conditions: SIP trunk architecture with soft switch. This bug affects both 12.4(15)T and 12.4(11)XW software releases.

  Workaround: A patch is required, forcing the media off when a busy message is received.

- CSCsr18605

  Symptoms: There was a build failure for c7200-p-mz referencing a header file in a wrong directory.

  Conditions: This bug implemented a change to the location of a file.

  Workaround: There is no workaround.

  Further Problem Description: This bug implemented a change to the location of an include file named errno.h that EEM requires in order to compile. The dsgs_cbs2 branch places errno.h in a different location than other branches. Thus EEM was required to make a change that fixed the build breakage in the dsgs_cbs2 branch. The effect of this change is that there is no difference in any branch other than dsgs_cbs2 and no executable code was altered.

  You can be assured that you do not need this bug for customer.

- CSCsr19440

  Symptoms: A router crashes if the **zone cluster local** command is configured with a cluster ID that is an empty string.

  Conditions: This symptom is observed when the local cluster ID and the local zone associated with the cluster are an empty string and when the **no service alignment detection** command is configured.

  Workaround: Configure the local cluster ID and the local zone associated with the cluster with a nonempty string. Also, configure the **service alignment detection** command to prevent the crash.

- CSCsr23975

  Symptoms: Build breakage occurs with -Wuninitialized flag in ips_base.c and ips_sme_service_smb.c.

  Conditions: This symptom is observed when the -Wuninitialized flag is used.

  Workaround: Use -Wno-uninitialized.

- CSCsr46333

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

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.4(20)T. This problem has been seen on only one router, and it happened only once. At this stage, the root cause has not been identified. This enclosure will be updated as more information is gathered.

  Workaround: There is no workaround.

- CSCsr49316

  Symptoms: A crash happens when the **show ipv6 rpf x:x:x::x** command is given.

  Conditions: This symptom is observed only when there are more than 16 adjacencies for a single static route. The crash happens when the **show ipv6 rpf** command is given for this particular static route.

  Workaround: There is no workaround. This problem occurs as long as there are more than 16 adjacencies for single static route even if some of them are not active.

- CSCsr50548

  Symptom: The zone-based firewall is dropping conference calls.

  Conditions: Make a conference call within the CCM. Conference resources are available out of the box, where the firewall is configured between the CCM and the conference resource GW. These conference resources are registered with CCM. Registration traffic is seen via the Skinny protocol. During a conference call, logs show that the firewall is dropping media packets.

  Workaround: There is no workaround.

- CSCsr50821

  Symptoms: A router may crash when ARP hits through interrupt level.

  Conditions: This symptom is observed when bridging is configured, but it may also be observed when the ARP code hits by interrupt context, which is unpredictable.

  Workaround: There is no workaround.

  Further Problem Description: This defect was introduced via CSCsq05997. Cisco IOS Release 12.4 and 12.4T are not affected by this defect, but Cisco IOS Release 12.2S may be affected by this defect.

- CSCsr55713

  Symptoms: A crash occurs.

  Conditions: The crash is caused by a ping across an ISATAP tunnel. The symptom is observed only in Cisco IOS Release 12.4(15)T7 on the Cisco 7200 (it is not known to affect other platforms), since the crash is dependent on the Cisco IOS memory map (which varies with each image).

  Workaround: There is no workaround.

- CSCsr55970

  Symptoms: A router may crash due to a bus error.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(20)T with a Cisco IOS firewall.

  Workaround: There is no workaround.

- CSCsr56105

  Symptoms: A Cisco IOS VoIP gateway may experience audio issues such as dead-air or one-way audio for a VoIP call present on the gateway. When this occurs, the following error message will be displayed on the gateway:

  ```
  %C5510-1-NO_RING_DESCRIPTORS: No more ring descriptors available
  ```

  Conditions: The symptom is observed on a Cisco 2801 VoIP gateway that is running Cisco IOS Release 12.4(20)T or Release 12.4(15)XZ1.

  Workaround: There is no known workaround to prevent this issue while using Cisco IOS Release 12.4(20)T or 12.4(15)XZ1 while using the Cisco 2801 router. Use an earlier release to avoid this issue.

- CSCsr56699

  Symptoms: A router crashes.

  Conditions: When invoking call features (hold, transfer, conf) on a CME router where the AIM-IPS-K9 (inline and prom) is configured on the tunnel interface, the router crashes due to a software-forced crash (corrupted next pointer blk) with a buffer overflow.

  Workaround: There is no workaround.

  Further Problem Description: How to reproduce the problem:

  1. IP phone A from Call Manager calls IP phone B belonging to the Cisco 3825 CME.
  2. Activating the call transfer button of IP phone B can crash the Cisco 3825 router.

  The normal call setup from the CM to the CME seems to be working fine.

  Other specifications:

  1. The problem can be reproduced without FW.
  2. The crash is reproduced with ids mon configured on the tunnel only (need not be on the G1/0.150 as in the original setup).
  3. Crash is reproduced in both promiscuous mode and inline mode. When ids mon is configured on the tunnel with one call up, simply put, the call on hold and the router will crash within a few seconds.
  4. The router does not crash if running in process mode.
  5. The crash is reproducible.
  6. The crash occurs if inline and bypass mode is configured.

7. This problem was found during follow-up workaround testing for CSCsq51416 where simple call is not able to complete if ids mon inline is configured only on the switch interface.

- CSCsr58052

  Symptoms: TCP packets with the Explicit Congestion Notificaton (ECN) bit turned on may be dropped by the Zone Based Firewall (ZBF), and the connection will not be established.

  Conditions: This symptom is observed when the TCP ECN bit is set on a new TCP connection in either direction (inbound or outbound) through the ZBF on the route.

  Workaround: Use Cisco IOS Release 12.4(15)T or an earlier release, as these releases are not affected.

  Further Problem Description: TCP ECN is described in RFC 3168.

- CSCsr59719

  Symptoms: A router may crash soon after the **cns config initial** command is configured.

  Conditions: The symptom is observed when the **cns config initial** command is configured with an invalid IP address for the status URL, for example:

  ```
  Router(config)# cns config initial non-existent-ip-address status
  http://1.1.1.1.1.1.1/junk
  ```

  When the connection to the initial server fails, the status message is posted to the status URL, which will cause the router to crash if the IP address is invalid.

  Workaround: Ensure that the configured IP addresses are valid.

- CSCsr64843

  Symptoms: A Cisco 1805 router may hang during reload.

  Conditions: This symptom is observed during the platform reload. After self-decompressing the image, the router goes into a hang state.

  Workaround: There is no workaround.

- CSCsr70197

  Symptoms: A router that is running Dynamic Multipoint VPN (DMVPN) may crash.

  Conditions: This symptom is observed when trying to unconfigure an MGRE tunnel interface that is running Next Hop Resolution Protocol (NHRP).

  Workaround: There is no workaround.

- CSCsr71715

  Symptoms: Call bubble may be missing, ringing LED may not be on, and Caller ID shows unknown.

  Conditions: These symptoms are observed after a hardware conference initiator parks or transfers the hardware conference call.

  Workaround: There is no workaround.

- CSCsr73798

  Symptoms: Traffic generated locally on the router in IVRF going to FVRF does not hit the crypto map and does not get encrypted. If the traffic arrives to the router from IVRF, everything works fine and packets are encrypted.

  Conditions: This symptom is observed when a crypto map is terminated in a front VRF in a router rather than in a global routing table. It is seen with packets that are generated locally on the router from an inside VRF that go to an outside VRF, and where there is a matching crypto map.

  Workaround: There is no workaround.

- CSCsr82003

  Symptoms: With a setup that has two routers receiving the same 300 multicast traffic from a video headend, if one of the links to the headend fails, about half of the multicast groups are blacked out as the RPF information for some of the sources is set wrong. Additionally, if both of the links are lost, we still have entries in the multicast routing table as the alternate route is used as the traffic incoming interface.

  The IGP is OSPF, with area0 in the core, and area 1 (to be set to stub soon) on the headend connecting links. There is MPLS TE with multicast-intact command under OSPF on the routers.

  Conditions: The problem happens when one of the headend connecting links is lost.

  Workaround: Remove the **ip multicast multipath** command from the two routers to disable ECMP load-splitting.

- CSCsr85766

  Symptoms: After an IP SLA operation finishes, all status variables that are expected to be conserved until the next operation become “Unknown.”

  Conditions:

  – If there is timezone offset and the local time date is advancing to the UTC date.

  – Found in Cisco IOS Release 12.4(20)T.

  Workaround: Schedule the operation so that it starts on the UTC date and the local date configured by the **clock timezone** command becomes the same.

- CSCsr87229

  Symptoms: Callers that use a caller-ID length of 15 characters or greater cannot call out of analog MGCP ports.

  Example:

  MGCP Packet received from --->
  CRCX 132 AALN/S0/SU1/0@nicmatth-ipipgw MGCP 0.1
  C: A0000000010000260000000F5
  X: 23
  L: p:20, a:PCMU, s:off, t:b8
  M: recvonly
  R: L/hd
  S: L/rg, L/ci(08/08/15/44,1002,This is my long name)
  Q: process,loop
  <---

  MGCP Packet sent to --->
  510 132 unsupported caller id length

  Conditions: The BELLCORE standards support only 15 characters, and the MGCP gateway disconnects the call because of unsupported caller-ID length and displays the following message:

  ```
  510 unsupported caller id length.
  ```

  Workaround: Configure a caller ID less then 15 character, or use the port with SCCP or H323 to prevent this. Also, the following cptones are not affected: FR, DE, NO, IT, ES, ZA, TR, GB, AT.

- CSCsr87466

  Symptoms: An outgoing INVITE from the Cisco IOS sip stack with SDP and authorization configured over the SIP trunk is failing because of an incorrect Response field generated within the Proxy Authorization header when the auth-int method is used as QOP. The Cisco IOS sip stack does not include SDP message body in the md5 hash calculation.

Conditions: This symptom is observed under the following conditions:

- Cisco IOS sip stack.
- The auth-int method is used.
- The outgoing INVITE packet contains SDP body.

Workaround: Potential workarounds are to:

- Disable early offer (not sure how to do it on IOS sip-ua).
- Use the auth method instead of the auth-int method. This should work if the incoming Proxy Authorization reply contains only the auth method.

- CSCsr93416

  Symptoms: The reflexive ACL implementation is broken (evaluated traffic is dropped by the return ACL).

  Conditions: This symptom is observed with Cisco IOS Release 12.4(20)T and only if the ACL with evaluate ACE (rule) has fewer than 13 ACEs (rules).

  Workaround: Add dummy rules (ACEs) to the ACL with an "evaluate" statement so that the number of rules (ACEs) in the ACL is greater than 13.

- CSCsr94563

  Symptoms: When registering an Embedded Event Manager (EEM) policy in a scheduler class that has no threads allocated to it, EEM will produce the following error message:

  ```
  %HA_EM-4-FMPD_NO_SCHED_THREAD: No threads are configured to service event class
  ```

  When attempting to unregister the policy, EEM may produce the following error and the policy will not be unregistered:

  ```
  EEM configuration: failed to unregister the event spec for policy policyname: unknown
  event ID
  ```

  In addition, a triggered event will not actually run once this problem is experienced.

  Conditions: This symptom is observed in images with the fix for CSCsr46367 and support for different scheduling classes in the EEM server.

  Workaround: First allocate some threads to the class, and then configure the policy in that class.

  Further Problem Description: This problem affects both Tcl-based policies and applets.

- CSCsu04446

  Symptoms: Cisco router running PfR Master Controller crashes under stress.

  Conditions: Traffic with more than 2000 prefixes with about 500 unreachable prefixes is flowing through the router.

  Workaround: This problem should not occur if you minimize the number of prefixes learned during an interval. The default of 100 should be sufficient.

  ```
  oer master
   learn
    prefixes 100
  ```

- CSCsu22997

  Symptoms: Right after executing the **show ephone summary** command, the device crashes due to a Bus Error (CPU signal 10).

  Conditions: Cisco 2811 running Cisco IOS Release 12.4(20)T with ephone.

  Workaround: There is no workaround.

- CSCsu31042

  Symptoms: A small memory leak may occur.

  Conditions: PPPoE or PPPoA client configured.

  Workaround: There is no workaround.

- CSCsu31444

  Symptoms: BR continuously displays error messages on the console.

```
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
%Error: timeout value is less than threshold 5000
```

  OER jitter probes are not created due to the above error.

  Conditions: Jitter probe configuration below for VOIP optimization.

```
oer-map BRANCH 20
 match traffic-class access-list Optimize_Voice_Traffic
 set mode route control
 set mode monitor fast
 set resolve mos priority 1 variance 30
 set resolve delay priority 2 variance 30
 set active-probe jitter 10.100.10.1 target-port 1025 codec g729a <<
 set probe frequency 4
```

  Workaround: There is no workaround.

- CSCsu31954

  Symptoms: A router reloads.

  Conditions: Under certain crytpo configurations with NetFlow also configured, the router will reload when required to fragment CEF-switched traffic on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsu33185

  Symptoms: Transmitted packets/bytes are zero, while packets are classified.

  Conditions: Configure the class map and policy map with the **random-detect ecn** command and apply the service policy on outbound serial interface. It is specific to the **random-detect ecn** command.

  Workaround: There is no workaround.

- CSCsu33399

  Symptoms: HWIC-4SHDSL:4Wire annex F/G with coding 16/32 TCPAM link on CO side down.

  Conditions: 4-WIRE SHDSL card with F/G annex-coding 16/32 TCPAM link on central office (CO) side going down. CO link goes down immediately at the moment either F/G annex configured and never comes up. But the link in CPE side will come up.

  - Issue seen with F/G annex; issue not seen with A/B annex.
  - CO side link goes down, but CPE comes up.

  Workaround: There is no workaround.

- CSCsu36827

  Symptoms: CUE clock does not synch up with the CME using NTP.

  Conditions: When UC500 is configured as NTP master.

  Workaround: Use external NTP server other than UC500.

- CSCsu45608

  Symptoms: A zone-based firewall does not allow returned TCP traffic from a VPN tunnel.

  Conditions: This symptom is observed when the firewall is configured to inspect TCP traffic to and from the VPN tunnel.

  Workaround: There is no workaround.

- CSCsu47037

  Symptoms: A router crashes when an attempt is made to forward a packet out of an Auto-Template interface. This occurs because the interface's MTU is set to 0. The **show interface Auto-Template X** command displays an MTU of 0.

  Conditions: This symptom is observed when an attempt is made to forward a packet out of an Auto-Template interface.

  Workaround: Configure a protocol MTU directly on the Auto-Template interface (that is, **ip mtu XXXX**).

- CSCsu51095

  Symptoms: If connected routes are optimized using PfR, there will be a routing loop.

  Conditions: This symptom can occur if for some reason pfr is learning connected routes or if the user has configured them.

  Workaround: The workaround is to create an oer-map with a prefix-list that contains the prefixes with ip addr of the connected routes (next hops). Set the set observe mode in the oer-map.

- CSCsu61741

  Symptoms: The **lsp ping** command is missing.

  Conditions: This issue is specific to the Cisco 7301.

  Workaround: There is no workaround.