Caveats for Cisco IOS Release 12.4T

September 04, 2013

Cisco IOS Release 12.4(24)T10

Text Part Number OL-8003-09 Rev. Z0

This document lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.4T, up to and including Cisco IOS Release 12.4(24)T10. Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

Because Cisco IOS Release 12.4T is based on Cisco IOS Release 12.4, many caveats that apply to Cisco IOS Release 12.4 will also apply to Cisco IOS Release 12.4T. For information on severity 1 and severity 2 caveats in Cisco IOS Release 12.4, see the Caveats for Cisco IOS Release 12.4 document located on Cisco.com.

To improve this document, we would appreciate your comments. If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically at http://www.cisco.com/feedback/ or contact caveats-doc@cisco.com. For more information, see the "Obtaining Documentation and Submitting a Service Request" section on page 1437.

Contents

- How to Use This Document, page 2
- If You Need More Information, page 2
- Resolved Caveats—Cisco IOS Release 12.4(24)T10, page 3
- Resolved Caveats—Cisco IOS Release 12.4(24)T8, page 4
- Resolved Caveats—Cisco IOS Release 12.4(24)T7, page 9
- Resolved Caveats—Cisco IOS Release 12.4(24)T6, page 17
- Resolved Caveats—Cisco IOS Release 12.4(24)T5, page 38
- Resolved Caveats—Cisco IOS Release 12.4(24)T4, page 50
- Resolved Caveats—Cisco IOS Release 12.4(24)T3, page 71
- Resolved Caveats—Cisco IOS Release 12.4(24)T2, page 91

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

- Resolved Caveats—Cisco IOS Release 12.4(24)T1, page 122
- Open Caveats—Cisco IOS Release 12.4(24)T, page 161
- Resolved Caveats—Cisco IOS Release 12.4(24)T, page 166
- Resolved Caveats—Cisco IOS Release 12.4(22)T5, page 239
- Caveats for 12.4(20)T1 through 12.4(22)T4, page 243
- Caveats for 12.4(15)T9 through 12.4(20)T, page 583
- Caveats for 12.4(9)T3 through 12.4(15)T8, page 823
- Caveats for 12.4(2)T through 12.4(9)T2, page 1125

How to Use This Document

This document describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The "Open Caveats" section lists open caveats that apply to the current release and may apply to previous releases.
- The "Resolved Caveats" sections list caveats resolved in a particular release, but open in previous releases.

Within the sections, the caveats are sorted alphanumerically by caveat number. The following information is provided for each caveat:

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

If You Need More Information

Cisco IOS software documentation can be found on the web through Cisco.com. For information on Cisco.com, see the "Obtaining Documentation and Submitting a Service Request" section on page 1437.

For more information on caveats and features in Cisco IOS Release 12.4T, refer to the following sources:

- Bug Toolkit—If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, l**og in** to Cisco.com and click **Products and Services: Cisco IOS Software: Cisco IOS Software Releases 12.2: Troubleshooting: Bug Toolkit**. Another option is to go to:

  http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

  (If the defect that you have requested cannot be displayed, this may be due to one of more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)
- Release Notes for Cisco IOS Release 12.4T—These release notes describe new features and significant software components for Cisco IOS software Release 12.4T.
- Deferral Advisories and Software Advisories for Cisco IOS Software—*Deferral Advisories and Software Advisories for Cisco IOS Software* provides information about caveats that are related to deferred software images for Cisco IOS releases. If you have an account on Cisco.com, you can access *Deferral Advisories and Software Advisories for Cisco IOS Software* at http://www.cisco.com/cisco/software/navigator.html

Note Release notes are modified only on an as-needed basis. The maintenance release number and the revision date represent the last time the release notes were modified to include new or updated information. For example, release notes are modified whenever any of the following items change: software or hardware features, feature sets, memory requirements, software deferrals for the platform, microcode or modem code, or related documents.

The most recent release notes when this caveats document was published were Release Notes for Cisco IOS Release 12.4T, for Cisco IOS Release 12.4(24)T10, published on September 04, 2013.

Resolved Caveats—Cisco IOS Release 12.4(24)T10

- CSCta87058

  Symptom: 5400XM gateway with 512MB memory, running CVP Post and routing SIP calls as an Ingress gateway, crashed with memory fragmentation after an uptime of 8 days. Trace from the core dump.

  Conditions: This symptom is observed with Cisco AS5400XM (BCM) processor (revision 0x22) with 393215K/131072K bytes of memory.

  ```
  Pool: Processor Free: 24101684 Cause: Memory fragmentation Alternate Pool: None Free:
  0 Cause: No Alternate pool -Process= "VTSP", ipl= 0, pid= 226, -Traceback= 0x606B3970z
  0x606D0DB4z 0x60C87FD8z 0x60C90098z 0x 60C88F58z 0x633A8744z 0x60C7EC98z 0x61F47A40z
  0x61F47BB8z 0x61E12158z 0x622C0094z 0x622C5120z 0x622C A870z 0x63033408z 0x63033CD0z
  0x622C6C34z
  Jul 18 19:07:30.360: %SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for ISDN
  Large Chu. No memo ry available -Process= "Chunk Manager", ipl= 3, pid= 1, -Traceback=
  0x6068C368z 0x6068C34C
  ```

  Workaround: There is no workaround.

- CSCtb43918

  Symptom: Router crashes at **ccsip_show_call_walker** with the issuing of “show sip calls” when active calls are present.

  Conditions: Router crashes on issuing of “show sip calls” when options is configured.

  Workaround: There is no workaround.

- CSCuc12685

  Symptoms: Address Error exception is observed with ccTDUtilValidateDataInstance.

  Conditions: This symptom is observed with ccTDUtilValidateDataInstance.

  Workaround: There is no workaround.

- CSCuc95160

  Symptoms: After receiving the CRCX message, *Cisco AS5400 does not send 200 ok to SSW*, SSW sends the CRCX message to the Cisco AS5400 again. Between these messages, debug outputs are displayed. It may seem that the call is not disconnected completely for the end point by the previous disconnect request (the DLCX is received after the CRCX message from SSW). The end point may be stuck in call_disconnecting state.

  Conditions: This symptom is observed with MGCP. This issue occurs when the Cisco AS5400 receives DLCX before sending “200 ok” for the first CRCX message.

  Workaround: There is no workaround.

- CSCue48419

  Symptoms: The Cisco AS5350 stops processing calls on PRI with a signaling backhaul from PGW. In the packet trace, there is no q931message from PGW. Further analysis shows that AS5350 sends a q_hold (0x5)message in BSM, causing peer (PGW) to stop sending signaling traffic. However, there is no BSM_resume message or BSM_reset sent after it. Hence, PGW is stuck in this condition. There was earlier defect for CSCts75818 with similar symptoms in U-state.

  Conditions: This symptom is observed due to some RUDP timing issues that cause BSM session switchover.

  Workaround: Reload the Cisco AS5350 (but only when CU notices the outage). Also, shutting both Ethernet interfaces may help, but this workaround has not been tested.

Resolved Caveats—Cisco IOS Release 12.4(24)T8

Cisco IOS Release 12.4(24)T8 is a rebuild release for Cisco IOS Release 12.4(24)T. The caveats in this section are resolved in Cisco IOS Release 12.4(24)T8 but may be open in previous Cisco IOS releases.

- CSCsz20655

  Symptoms: Policy-map gets detached from the interface when bandwidth changed to allowable (policy-map) range and attachable to the same bandwidth again. There is no change in policy-map either when the policy-map gets detached from the interface.

  The policy-map gets detached with an error message “CBWFQ: Removing service policy on GigabitEthernet0/1”. However, the policy-map is attachable to the same interface bandwidth.

  Problem Impact: Policy-map is getting removed from interface.

  Root Cause:

```
72b#sh policy-map td
  Policy Map td
    Class class-default
      bandwidth 60 (kbps)
      service-policy tdc
72b#sh policy-map tdc
  Policy Map tdc
    Class ip-prec3
      bandwidth 20 (kbps)
    Class class-default

-
qosde-rckf8-72(config-if)#bandwidth 1000
[HQF-ADMIT-EVENT] hqf_admit_layer_minrate_kbps: layer: 0x66F937C4, layertype:
4, kbps: 1000
AKS_DEBUG:layertype: 4, kbps: 1000, perc
AKS_DEBUG:layertype: 4, kbps: 6, perc: 60           <<<<<<<<<<< Here it is
falling into BW percentage case even though absolute BW is configured in
parent.
[HQF-ADMIT-EVENT] hqf_admit_layer_minrate_kbps: layer: 0x66F9377C, layertype:
8, kbps: 6
```

```
[HQF-ADMIT-ERROR] hqf_admit_layer_minrate_kbps: Failed: total required: 21
kbps                      <<<<<<<< Ref BW passed to child during the
recursive call is wrong.
%QOS-4-INVALIDBW: interface Ethernet4/1: Not enough bandwidth to configure
service-policy

[HQF-ADMIT-EVENT] hqf_admit_minrate_kbps: layer: 0x0, blt: 0x66E08E00 (flags:
0x20220004), old kbps: 20, new kbps: 20, ref rate: 60
[HQF-ADMIT-EVENT] hqf_admit_minrate_kbps: layer: 0x0, blt: 0x66E08F80 (flags:
0x20220004), old kbps: 60, new kbps: 60, ref rate: 1000
qosde-rckf8-72(config-if)#do sh policy-map tdc
-
In hqf_admit_minrate_kbps API,
          if (blt->perc) {                 <<<<< It is falling into this case
even though no bandwidth % config in policy.
                tmp_kbps = (ulong)ULONGLONG_2MULTIPLIER_1DIVISOR(blt->perc,
                                  ref_rate_kbps,
                                  HQFLAYER_TOTAL_PERCENT_SCALED);
            } else if (IS_LOGICAL_LAYER(layertype)) {
                tmp_kbps = ref_rate_kbps;
            } else if (IS_LOGICAL_LAYER(curlayer->layertype)){
                tmp_kbps = ref_rate_kbps;
            } else if (hqf_is_implicit_minrate_queue(blt)) {
                /*
                 * we want to check if it is LOGICAL layer first
                 * before we check for implicit minrate queues
                 */
                tmp_kbps = implicit_minrate;
            } else {
                /*
                 * skip this blt         <<< should fall in this case when
absolute BW is configured.
                 */
                continue;
            }
```

Fix Description: As per the HQF architecture, blt->perc is set even though no bandwidth %. Show hqf int is also shows the percent value. So, checking blt- >perc is not enough also check HQF_IS_BLT_FLAG_SET(blt, HQF_BANDWIDTH_PERCENT) and if that is the case then and then calculate the absolute rate from the percent value.

Workaround: There is no workaround.

- CSCth20872

  Symptoms: The following error message is seen accompanied by a reset of the Fast Ethernet:

  ```
  %C870_FE-3-TXERR: FastEthernet0: Fatal transmit error. Restarting...
  ```

  Conditions: The symptom is observed on a Cisco 877 router that is running Cisco IOS Release 12.4(24)T3.

Workaround: There is no workaround.

- CSCti75666

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

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

  Workaround: Convert H.323 leg to SIP.

- CSCtj48387

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

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

  Workaround: There is no workaround.

  Further Problem Description: This fix needs to be included in the Cisco ME 3400.

- CSCtj59117

  Symptoms: The following error message is seen and the router freezes and crashes:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle
  ```

  A reload is required to recover.

  Conditions: The symptom is observed on a Cisco 1803 that is running Cisco IOS Release 12.4(15)T12 or Release 12.4(15)T14.

  Workaround: Remove CEF.

- CSCtj79476

  Symptoms: Traffic loss and VLAN related errors are seen when the traffic is sent for a prolonged duration on an HWIC.

  Conditions: The symptom is observed when traffic is sent for a prolonged duration (over 12 hours) on an HWIC.

  esw_mrvl_vlan_port_remove : Unable to find entry for VLAN(50) dbnum(3)

  esw_mrvl_vlan_port_remove : Unable to find entry for VLAN(52) dbnum(4)

  The following devices are affected.

  - HWIC-4ESW
  - HWIC-4ESW-POE
  - HWIC-D-9ESW
  - HWIC-D-9ESW-POE

  Workaround: Delete the VLAN and create it back. Will not work on VLAN 1 as we cannot delete VLAN 1 from database.

  Further information: If you upgrade, please also make sure that you avoid the following similar bug:

  CSCtx72953 Traffic loss on hwic-4ESW due to loss of VLAN.

- CSCtr86328

  Symptoms A device running Cisco IOS might reload when the web browser refreshes/reloads the SSL VPN portal page.

Conditions: Cisco IOS device configured for clientless SSL VPN.

Workaround: There is no workaround.

Further Problem Description: This problem has been seen when the stock Android browser visits the SSL VPN portal (after authentication) and refreshes (reloads) the page. However, the issue is not browser-specific and other browsers might trigger the issue too.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/6.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:U/RC:C

CVE ID CVE-2012-1344 has been assigned to document this issue.

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

- CSCtt94391

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

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

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

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

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8:

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

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

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

- CSCtu16433

  Symptoms: A Cisco router may reload due to a bus error. It appears to reload just after registration:

  ```
  %GDOI-5-GM_REGS_COMPL: Registration to KS <snip> complete for group <snip> using
  address <snip>
  ```

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = <snip>
  ```

  Conditions: The symptom is observed using GET VPN on Cisco IOS Release 12.4T, 15.0, or 15.1. Cisco IOS Release 15.2 is not affected.

  Workaround: There is no workaround.

- CSCtw55976

  Cisco IOS Software contains a vulnerability in the Intrusion Prevention System (IPS) feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if specific Cisco IOS IPS configurations exist.

  Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available.

This advisory is available at the following link:

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

- CSCtx72953

  Symptoms: During normal operation, traffic is lost on the HWIC-4ESW and some VLAN information is missing. In the logs you see:

  ```
  esw_mrvl_vlan_port_remove : Unable to find entry for VLAN(xxx) dbnum(xxx)
  ```

  and/or:

  ```
  esw_mrvl_vlan_port_untagged : Unable to find entry for VLAN(1)
  ```

  Conditions: The symptom is observed with Cisco IOS Release 15.1(4)M3.

  Workaround: Delete/recreate lost VLAN (except VLAN 1).

- CSCty58992

  Symptoms: One-way audio is observed after transfer to a SIP POTS Phone.

  Conditions: This symptom is observed under the following conditions:

  - Cluster is in v6 mode.
  - A call is made from Phone1 to Phone2, and then Phone2 transfers the call to Phone3(SIP POTS), which is when the issue occurs.

  Workaround: There is no workaround.

- CSCty80074

  Symptoms: A Cisco 3800 router running Cisco IOS Release 15.0(1)M7, with only Multilink or Serials, shows aborts and input errors during normal traffic conditions.

  Conditions: This symptom is observed with normal traffic load. In addition, when a ping sweep is done, aborts and input errors are seen more frequently.

  Workaround: There is no workaround.

- CSCtz27137

  Symptoms: An upgrade to the S639 or later signature package may cause a Cisco IOS router to crash.

  Conditions: This symptom is observed in a Cisco 1841, 1941, and 2911 router running one of the following Cisco IOS versions:

  - Cisco IOS Release 12.4(24)T4
  - Cisco IOS Release 15.0(1)M4
  - Cisco IOS Release 15.0(1)M8
  - Cisco IOS Release 15.2(3)T

  Workaround: Update the signature package to anything less than S639. If already updated with any package larger than or equal to S639, follow the below steps to disable IPS:

  - Access the router via the console.
  - Enter break sequence to access ROMmon mode.
  - Change the config-register value to 0x2412.
  - Boot the router to bypass the startup-configuration.
  - Configure the basic IP parameters.

  - TFTP a modified configuration to the router's running-configuration with Cisco IOS IPS disabled.
  - Reset the config-register to 0x2102.
  - Enter the **write memory** command and reload.

- CSCtz47595

  Symptoms: Dial string sends digits at incorrect times.

  Conditions: The symptoms are seen with a Cisco 3925 router running Cisco IOS Release 15.2(3)T using PVDM2-36DM modems with firmware version 3.12.3 connecting over an ISDN PRI to an analog modem.

  When using a dial string to dial an extension (or other additional digits), the modem should answer before the dial string is sent. If a comma is used, there should be a pause after connecting before sending the digits. The default value of the digital modem is one second per comma; two commas would be two seconds, three commas = three seconds and so on.

  1. With any number of commas in the string, debugs show the digits are sent at random intervals, sometimes before the call was answered and as much as up to 30 seconds after the call connects, i.e.: 919195551212x,22 or 1212x,,,22.
  2. With no comma in the dial string, the digits are sent immediately after being generated without waiting for a connection, i.e.: 919195551212x22.

  Dialing directly to a number with no extension or extra digits works as expected.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.4(24)T7

Cisco IOS Release 12.4(24)T7 is a rebuild release for Cisco IOS Release 12.4(24)T. The caveats in this section are resolved in Cisco IOS Release 12.4(24)T7 but may be open in previous Cisco IOS releases.

- CSCtg06045

  Symptoms: A Cisco router may reload with traceback from a crypto ACL configuration.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.4(15)T12 and experiencing a high CPU stress load while the ACEs are being changed periodically. This symptom is specific to the ACE entries in crypto ACL downloaded from KS.

  Workaround: Simplify and consolidate the ACE entries in the crypto ACL. In addition, reducing the CPU stress level may help.

- CSCtg47129

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

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

  This advisory is available at the following link:

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

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

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

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

- CSCtg83804

  Symptoms: Router crashes when uploading or downloading files via WebVPN.

  Conditions: This symptom is observed on a Cisco 870 router, WebVPN, and BVI configuration.

  Workaround: There is no workaround.

- CSCti10222

  Symptoms: The following exceptions are seen:

```
%SYS-2-MALLOCFAIL: Memory allocation of XXXX bytes failed from 0xYYYYYYYY,
alignment # Pool: I/O  Free: #  Cause: Memory fragmentation Alternate Pool:
None  Free: 0  Cause: No Alternate pool
-Process= "IGMP Snooping Receiving Process", ipl= #, pid= #,  -Traceback=
0x81E8B6BCz 0x81EB0660z 0x802EC198z 0x802EC8E4z 0x802ED88Cz 0x802F1988z
0x803BBD88z 0x803BBF2Cz 0x8045E5CCz 0x804615F4z

 Can't duplicate packet
 Can't duplicate packet
 Can't duplicate packet
```

  Conditions: This symptom is observed when VLANs are added while multicast traffic is flowing through the router.

  Workaround:

  1. Prune the multicast feed that is coming from the respective VLAN using the **switchport trunk allowed vlans except** *mcast vlan#* command.

  or

  2. Upgrade to Cisco IOS Release 15.1(2)T1.

- CSCti35326

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

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

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

  This advisory is available at the following link:

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

- CSCti46171

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

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

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

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

- CSCtj33003

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

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

  This advisory is available at the following link:

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

- CSCtl20508

  Symptoms: A Cisco router fails to decrypt a packet, and for all packets received, the following message is logged:

  ```
  IPSEC(epa_des_crypt): decrypted packet failed SA identity check
  ```

  In the “sh crypto ipsec sa”, the counter that increases is the “#recv errors’’.

  Conditions: This symptom is observed on a Cisco 3270 router that is running Cisco IOS Release 15.0(1)M4. The tunnel interface has a crypto ipsec profile. Transport mode is being used. Packets received on this tunnel are not properly decrypted.

  This issue is not observed when reverting to default tunnel mode.

  Workaround: There is no workaround.

- CSCtn16855

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

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

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

- CSCtn76183

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

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

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

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

- CSCtn83520

  Symptoms: VOIP_RTCP related traceback is seen.

  Conditions: This symptom is observed when IPIP gateways are involved.

  Workaround: There is no workaround.

- CSCto32044

  Symptoms: The interface hangs and fails to pass traffic. It will still show an "up/up" status but the input and output rates will go to 0. The following errors will be seen:

```
%SBETH-3-ERRINT: GigabitEthernet0/0, error interrupt, mac_status = 0x0000040000000000
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to reset
```

  The interface number will vary.

  Conditions: The conditions are unknown.

  Workaround: There is no workaround.

- CSCto72927

  Symptoms: Configuring an event manager policy may cause a Cisco router to stop responding.

  Conditions: This issue is seen when a TCL policy is configured and copied to the device.

  Workaround: There is no workaround.

- CSCtq45553

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

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

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

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

- CSCtq55173

  Symptoms: A device that is configured with NAT crashes. SIP appears to be translated trough NAT. However, some cases report that the crash still occurs after redirecting SIP traffic elsewhere.

  Conditions: The crash is triggered when the **clear ip nat translation** *, **clear ip nat translation forced**, or **clear crypto ipsec client ezvpn** command is entered.

  Workaround: There is no workaround.

- CSCtq63838

  Symptoms: A Cisco 2921 router crashes, and the following traceback is seen:

```
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback=
0x24A19810z 0x24A5DC8Cz 0x24A4A560z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
0x233DEA40z 0x233DEA24z
```

```
ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1528: unkn -Traceback=
0x24A19810z 0x24A5DC8Cz 0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z
0x233DEA40z 0x233DEA24z
```

```
%SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 315556E0. -Process= "DSMP",
ipl= 0, pid= 306, -Traceback= 0x246EBB2Cz 0x24719984z 0x24A19810z 0x24A5DC8Cz
0x24A4A7E0z 0x24DF6618z 0x24DF6BBCz 0x24A2DD5Cz 0x24A2E274z 0x233DEA40z 0x233DEA24z
23:50:00 UTC Sun May 1 2011: TLB (load or instruction fetch) exception, CPU signal
10, PC = 0x2581FB94
```

Conditions: This symptom is observed with the DSMP process.

Workaround: There is no workaround.

- CSCtr28857

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

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

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

- CSCtr29338

  Symptoms: A router crashes.

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

  Workaround: There is no workaround.

- CSCtr54327

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

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

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

- CSCtr83533

  Symptoms: When you check the message on a VM system and that triggers the SIP notify to turn off the MWI to IAD, IAD will turn off the MWI but, after that, DSP is not released for the port. If you make one more call, in the next call you will hear silence. After it is off hook, there is no ring tone.

  Conditions: The symptom is observed when MWI is configured for analog ports on IAD, and if MWI is ON and a call is made to clear the MWI.

  Workaround 1: Reload the router.

  Workaround 2: Remove the MWI configuration from the analog port configuration.

- CSCtr83659

  Symptoms: GETVPN group members stop communicating with each other after a partial network outage.

  Conditions: This symptom is seen when a MPLS outage occurs with the following characteristics:

  - Traffic flow stop between KS-1 and KS-2
  - KS-2 can send rekey to GM-1 and GM-2. However, ACKs from these two GMs cannot reach KS-2.

  Outage does not need to be MPLS related.

  Workaround: There is no workaround.

- CSCtr91106

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

  This advisory is available at the following link:

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

- CSCtr97640

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

  Conditions: None.

  Workaround: None--Physically securing the router is important.

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

  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:U/RC:C CVE ID CVE-2011-3289 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCts24348

  Symptoms: PBR "set vrf" feature can cause unnecessary ARP requests and packet drops if some other feature is configured on the same router interface and packets are punted to process-switching path. This issue slows down TCP traffic considerably as first SYN in a flow may always be dropped.

  Conditions: The symptom is observed with multi-VRF selection using the Policy Based Routing (PBR) feature. It was observed in all IOS versions with new CEF code (Cisco IOS Release 12.4(20)T and upwards). The issue was not seen in Cisco IOS Release 12.4(15)T and Release 12.4(25).

  Workaround: This issue can be alleviated by using proxy ARP on the upstream device. Otherwise, there is no workaround.

- CSCts33952

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

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

  Workaround: There is no workaround.

- CSCts38429

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

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

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

- CSCts59014

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

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

  Workaround: There is no workaround.

- CSCts76410

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

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

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

- CSCts85251

  Symptoms: Router with GETVPN enabled may experience high CPU and memory exhaustion leading to a crash.

  Conditions: This symptom was first seen on Cisco IOS Release 12.4(24)T5 but is not exclusive to it.

  Workaround: There is no workaround.

- CSCtt97905

  Symptoms: Multiple demandNbrCallDetails traps generated.

  Conditions: This symptom is seen when multiple demandNbrCallDetails traps are generated for connect under normal conditions.

  Workaround: There is no workaround.

- CSCtu02835

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

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

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

- CSCtu21636

  Symptoms: Sometime calls are dropped if there are active calls on the DSP. The following errors are displayed in the logs:

  ```
  Power alarm on DSP channel ch=1 is ON 0001 0001 **
  Power alarm on DSP channel ch=1 is OFF 0001 0000 **
  Power alarm on DSP channel ch=1 is ON 0001 0001 **
  Power alarm on DSP channel ch=1 is OFF 0001 0000 **
  ```

Conditions: This symptom is seen with all conditions.

Workaround: There is no workaround.

- CSCtw66863

  Symptoms: A Cisco router may crash when using VXML script with Cisco proprietary tag *Cisco-data*.

  Conditions: This symptom is observed when the *Cisco-data* tag uses memory beyond allocated, which causes router to crash intermittently.

  Workaround: There is no workaround.

- CSCtx38806

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

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

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

  ```
  "The page isn't redirecting properly"
  ```

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

  Workaround: Any of the following workarounds will work:

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

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

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

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

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

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

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

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

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

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

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

Resolved Caveats—Cisco IOS Release 12.4(24)T6

Cisco IOS Release 12.4(24)T6 is a rebuild release for Cisco IOS Release 12.4(24)T. The caveats in this section are resolved in Cisco IOS Release 12.4(24)T6 but may be open in previous Cisco IOS releases.

- CSCsl24511

  Symptoms: The problem was introduced due to the existence of multiple outgoing mcast interfaces. When ToS was changed from one interface during particle-based fast switching, the change was carried to other interfaces, which made the QoS policy perform incorrectly.

  Conditions: The fix should be applied to Cisco IOS Releases 12.2SR and 12.2SX. The reported issue is not seen in haw_t, however, because it will fix CSCtj49957, which was duplicated from this DDTS. This fix should also be committed to the T-train and all other major branches that are *not* using MFIB forwarding.

  Workaround: Disable fast switching and do process switching only.

- CSCsm87925

  Symptoms: A memory leak occurs in SSGCmdQue.

  Conditions: This symptom occurs on routers that are configured for Service Selection Gateway (SSG) and that are running Cisco IOS Release 12.4(15)T2.

  Workaround: There is no workaround.

- CSCso33003

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

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

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

- CSCso46409

  Symptoms: mbrd_netio_isr and crypto_engine_hsp_hipri traceback log messages are produced.

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

  Workaround: There is no workaround.

- CSCsq27561

  Symptoms: A router may crash when changing the IP address of an interface that is a common IPsec endpoint for many tunnels.

  Conditions: This symptom has been seen only in ION so far and has not been reported in routers that are running Cisco IOS software.

  Workaround: To change the IP address on the VLAN that has been used as a common local IPsec endpoint address for thousands of IPsec SAs and tunnels, we recommend that the customer do the following:

  1) Shut down the physical and VLAN interfaces to stop traffic.

  2) Execute the **clear crypto session** command or the **clear crypto sa** command, followed by the **clear crypto isakmp sa** command.

  3) Change the IP address.

- CSCsv29916

  Symptoms: A router crashes.

Conditions: This symptom is observed when domain stripping with a VRF configuration is removed more than twice.

Workaround: There is no workaround.

- CSCsv73754

  Symptoms: A router crashes during VRF configuration. A traceback decode points to a function bgp_vpn_impq_add_vrfs_cfg_changes.

  Conditions: The symptom is observed while unconfiguring VRFs. It is most likely to be seen when 100 or more VRFs are unconfigured.

  Workaround: There is no workaround.

- CSCsv92961

  Symptoms: When bouncing the interface between PE and receiver CE, the traffic does not resume.

  Conditions: This symptom occurs on a multicast-enabled frame relay interface on a Cisco Edge Services Router (ESR) that is acting as an encap PE. It appears after using the **shutdown** command followed by the **no shutdown** command on the frame relay interface connected to the CE sending traffic. The multicast traffic stops passing through this interface. The CE is sending traffic continuously while the **shutdown** command followed by the **no shutdown** command operation is performed on the PE.

  Workaround: Stop traffic and wait for timers to expire. Start traffic again. The traffic flows through the interface.

- CSCsw32795

  Symptoms: The key server crashes during unconfiguration.

  Conditions: Occurs when all the configuration (including GDOI configurations) in the Primary KS is removed and then immediately the unconfiguration is done in the Secondary KS as well.

  Workaround: If you wait for a few minutes after the secondary transitions to the primary (after the Primary KS is down), then the crash will not be seen.

- CSCsw69621

  Symptoms: A BR goes down on the learning cycle.

  Conditions: The symptoms are observed when the inside BGP learning is configured:

  ```
  configure terminal
   oer master
    learn
     no throughput
     no delay
     inside bgp
  ```

  Workaround: Configure as follows:

  ```
  configure terminal
   oer master
    learn
     throughput
     inside bgp
  ```

- CSCsw70555

  Symptoms: A Cisco 1811 V.92 interface sees CRC errors against different modems using Pagent.

  Conditions: 50 PPS of 64-byte frames were being sent in each direction through the V.92 interface on the Cisco 181x.

Workaround: Configure the **no ppp microcode** command under the async interface.

- CSCsw99171

  Symptoms: The Xconnect feature does not function properly. Packets sent to an interface with **xconnect <peer router> 1 encapsulation mpls** configured are dropped.

  Conditions: The problem occurs only when Xconnect is configured on an interface.

  Workaround: Do not configure the Xconnect feature.

  Further Problem Description: Cisco 7300 platforms also do not support native vlan when Xconnect is configured on the same subinterface. See CSCee01032.

- CSCsx03120

  Symptoms: When an ATM interface on a WIC1-ADSL comes back up after a flap, under some undefined circumstances, it may be observed that none of the configured PVCs forward traffic.

  Conditions: Specific conditions are still under investigation.

  Workaround: Perform a **shut/no shut** on the interface or power-cycle the router.

- CSCsx49573

  Symptoms: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sr-20090114-http.shtml

  Conditions: See the "Additional Information" section in the posted response for further details.

  Workarounds: See the "Workaround" section in the posted response for further details.

- CSCsx75520

  Symptoms: Ping is not working on a Cisco router with a ctunnel interface.

  Conditions: This symptom is observed after attaching a policy map to a ctunnel interface.

  Workaround: Delete the policy map from the ctunnel interface using the **no policy-map** command and reload the router.

- CSCsy15098

  Symptoms: Cisco 3845 reloads at cm_destroy_connection while changing mode ATM AIM 0 to CAS.

  Conditions: Occurs while switching a Cisco 3845 with an existing connection.

  Workaround: There is no workaround.

- CSCsy22787

  Symptoms: Existing NBAR HTTP implementation does not do correct subport classification in some cases.

  Conditions: NBAR is used for HTTP subport classification.

  Workaround: There is no workaround.

- CSCsy26448

  Symptoms: Router configured with DNS crashes when deleting a trust-point.

  Conditions: The symptom is observed on a Cisco 7200 series and Cisco 3845 router that is running Cisco IOS Release 12.4(24.6)T.

Workaround: There is no workaround.

- CSCsy84798

  Symptoms: IPv6 classification is not working at the MFR interface.

  Conditions: This symptom is observed at the main MFR interface.

  Workaround: Attach at MFR point-point.

- CSCsz07103

  Symptoms: A router crashes at nvgen_action when 500 IPSec tunnels are configured and the **write memory** command is issued.

  Conditions: This symptom is observed when 500 IPSec tunnels are configured and the **write memory** command is issued. The problem might be a scalability issue.

  Workaround: There is no workaround.

- CSCsz18573

  Symptoms: A number of problems are found in the early version of the NEMO mobile router:

  - MR tunnel will flap with NEMO explicit prefix configured.
  - Roaming can be slow or fail installing routes.
  - MR routes appear as static as opposed to mobile.
  - Configuring the home address on a loopback is required.
  - ND operates on the MIP tunnel.
  - Ten seconds latency appears on MR at tunnel setup and on HA at roaming.

  Conditions: These symptoms occur when running Cisco IOS Release 12.4(22)T1 and Release 15.0(1)M.

  Workaround: There is no workaround.

- CSCsz39222

  Symptoms: The Cisco CMTS reloads and crash file indicates a cache error.

  Conditions: This issue is observed when register 26/0 contains 0xC0000000.

  This issue affects the NPE-G1 on a Cisco 7200 platform, and the PRE4 on a Cisco UBR10012 router. NPE-G2 is not affected. There is no specific trigger for this failure other than having a single bit parity error on ECC memory.

  Workaround: There is no workaround.

  Further Problem Description: This symptom does not cause a parity error or actually cause the crash. This symptom is just to add a error handler for the specific case of a single bit correctable parity error in ECC memory. The crash results from the parity error itself. The following is an example of the beginning of a crashinfo collection for a hardware corrected cache error:

  ```
  Cache error detected! CPO_ECC (reg 26/0): 0xC0000000 CPO_CACHERI (reg 27/0):
  0x34001DE0 CPO_CACHERD (reg 27/1): 0x10800580 CPO_CCHEDPA (reg 27/3): 0x017B4580
  ```

- CSCsz44220

  Symptoms: Passive FTP flows are not classified by NBAR if they are translated by NAT.

  Conditions: The symptom is observed under the following conditions:

  1. It is seen in both directions: input and output.

  2. It is verified with fast Ethernet, ATM PVC, serial and dialer interface only.

3. It is observed with Cisco IOS T train releases only.

Workaround: Use Cisco IOS mainline code.

- CSCsz89093

  Symptoms: A Cisco 2800 router may drop multicast packets.

  Conditions: This symptom is observed when stream sources are connected to an NM-16ESW switch module.

  Workaround: Disable IGMP snooping.

  Further Problem Description: Packet loss can be seen with as little as 1 stream consisting of 1500 byte packets @ >= 1470 pps. Packet loss can be viewed as follows:

  ```
  Router# show int Fa1/1 stat
  ```

  ```
  FastEthernet1/1 Switching path Pkts In Chars In Pkts Out Chars Out Processor 100000
  150000000 53 4028 Route cache 0 0 0 0 Total 100000 150000000 53 4028 <--- 100,000 pkts
  received
  ```

  ```
  Router# show int Vlan200 stat
  ```

  ```
  Vlan200 Switching path Pkts In Chars In Pkts Out Chars Out Processor 0 0 0 0 Route
  cache 99997 149595512 0 0 Total 99997 149595512 0 0 <--- 3 pkts dropped
  ```

- CSCsz97091

  Symptoms: Packet drop occurs when **show version**, **show run**, and **write memory** commands are issued.

  Conditions: Packet drop will be observed as input errors accounted as overruns. The rate of packets being dropped will be proportional to the rate of traffic.

  Workaround: There is no workaround.

- CSCta98321

  Symptoms: AAA server for HTTP authentication cannot be configured on a Cisco 861 integrated services router (ISR).

  Conditions: This symptom is observed when configuring the AAA server for HTTP authentication on a Cisco 861 ISR.

  Workaround: There is no workaround.

- CSCtb38975

  Symptoms: Updating the DHCP lease time with a new value has no effect.

  Conditions: This symptom occurs when the renewal process is forced.

  Workaround: There is no workaround.

- CSCtb56567

  Symptoms: A Cisco voice gateway experiences a memory leak error on CCSIP SPI CONTROL process, which may lead the router to crash every 4 to 5 days.

  Conditions: This symptom is observed when a router is configured with sip- ua using the **mwi-server** command with transport set to *tcp*, but the server specified is not set up to receive sip and thus replies with tcp resets. This can be caused by misconfigured sip mwi.

  Workaround: Reload the device regularly to free the memory.

- CSCtb56645

  Symptoms: COOP-KS functionality is broken after the commit of CSCsw32795.

Conditions: Run GETVPN COOP-KS functionality, and the primary-KS and secondary-KS relationship cannot be established.

Workaround: Do not use COOP-KS functionality.

- CSCtb66295

  Symptoms: No ip connectivity exists due to erroneous ARP tables.

  Conditions: This symptom is observed when NAT and HSRP are configured on the same interface.

  Workaround: There is no workaround.

- CSCtb70102

  Symptoms: When SRST and STCAPP are configured and running on the same router, SCCCP-controlled analog phones may be unable to make an outgoing call.

  Conditions: This symptom is observed when, upon WAN link failure, the phones register to an SRST gateway.

  Workaround: There is no workaround.

  Further Problem Description: This symptom occurs due to STCAPP automatically adding a *station-id* parameter under the **voice-port** command in order to save DN information for registration to SRST.

- CSCtb72734

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

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

  Workaround: There is no workaround.

- CSCtb74547

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

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

  Workaround: There is no workaround.

- CSCtb76775

  Symptoms: A Cisco 3900 series router may experience a large IO memory leak.

  Conditions: This symptom is observed with IPSec and QoS on a Cisco NM-1A- T3/E3 network module with NME-IPS in promiscuous mode.

  Workaround: Run IPS in inline mode.

- CSCtb83578

  Symptoms: A severe memory leak may occur on a Cisco CME router.

  Conditions: This symptom is observed on a Cisco CME router with the CCSIP- REGISTER process.

  Workaround: There is no workaround.

- CSCtc27454

  Symptoms: A Cisco router may crash after displaying the following CPUHOG message for the Crypto ACL process:

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

Conditions: This symptom is observed when the DMVPN tunnel is shut down.

Workaround: There is no workaround.

- CSCtc40477

  Symptoms: A Cisco router may crash after disabling then re-enabling NBAR on an interface.

  Conditions: This symptom is observed when policy-map classification based on NBAR and NAT is configured on the router.

  Workaround: Create a dummy subinterface and enable NBAR using the **ip nbar protocol-discovery** command.

  Alternate workaround: While migrating on the subinterface, disable NBAR using the **no ip nbar protocol-discovery** command on the old interface only after enabling NBAR on the newly-migrated interface.

- CSCtc42734

  Symptoms: A communication failure may occur due to a stale next-hop.

  Conditions: This symptom is observed when the static route for an IPv6 prefix assigned by DHCP has a stale next-hop for terminated users.

  Workaround: Reload the router.

- CSCtc68910

  Symptoms: Unnecessary retransmission and spurious TCP is reset.

  Conditions: The symptom is observed when using NAT and a large (already fragmented) "updatecabilitiesversion2" traverses the router.

  Workaround: There is no workaround.

  Further Problem Description: This problem seems to be correlated to:

  - IP phone presents an updatecabilitiesversion2 large packet (i.e.: 2012 bytes) fragmented (i.e.: in 4 pieces).

- CSCtc75789

  Symptoms: The **ip multicast boundary filter-autorp** command is not working properly.

  Conditions: The locally originated auto rp announce will have the wrong UDP checksum if the **ip multicast boundary filter-autorp** command is configured on an interface.

  Workaround: There is no workaround.

- CSCtc97687

  Symptoms: A mobile router (MR) cannot roam between two interfaces on the same access router or between two different access routers.

  Conditions: This symptom is observed on an MR with a single roaming interface roaming between two different interfaces on the access router or between two different access routers.

  Workaround: There is no workaround.

- CSCtd40613

  Symptoms: For packets that are destined to unresolved neighbors, CEF will either:

  1) Upon resolution failure: fail to send an ICMP unreachable containing (part of) the original packet that prompted the resolution.

  2) Upon resolution success: fail to send the original packet to the neighbor.

Conditions: This failure occurs when the driver has insufficient buffers to clone the original packet. It affects only some drivers. The list of affected drivers is not completely known.

Workaround: There is no workaround.

- CSCtd74470

  Symptoms: Voice ports on gateways configured for E1 R2 intermittently get stuck in the "clearfwd" state and can only be returned to normal operation mode by manual intervention.

  Conditions: When the issue occurs, the following states are observed by examining the stuck port with **show** commands:

```
Router# show vo po su | include clearfwd
0/3/0:1 24 r2-digital up up clearfwd idle y

Router# show voice trace 0/3/0.1.24
0/3/0:1 24 State Transitions: timestamp (state, event) -> (state, event) ...
3440023.272 (R2_Q421_IDLE, E_HTSP_SETUP_REQ) ->
3440023.380 (R2_Q421_OG_SEIZE, E_DSP_SIG_1100) ->
3440047.816 (R2_Q421_OG_SEIZE_ACK, E_R2_REG_ABORT_DIGIT_COLLECT) ->
3440047.816 (R2_Q421_OG_CLR_FWD, E_DSP_DIALING_DONE) ->
3440048.816 (R2_Q421_OG_CLR_FWD, E_HTSP_EVENT_TIMER) - >
3440050.816 (R2_Q421_WAIT_IDLE, E_HTSP_EVENT_TIMER) ->
3440050.816 (R2_Q421_WAIT_IDLE, E_DSP_SIG_1100) ->
3440050.820 (R2_Q421_BLOCKED, E_DSP_SIG_1100) ->
3440069.960 (R2_Q421_BLOCKED, E_HTSP_RELEASE_REQ) ->
3440113.512 (R2_Q421_BLOCKED, E_DSP_SIG_1000) ->) ->
```

  Workaround: Shut/no shut the controller or busy-out the channel:

```
Router# show vo po sum | include clearfwd
0/3/0:1 24 r2-digital up up clearfwd idle y
0/2/0:1 21 r2-digital up up clearfwd idle y
0/2/0:1 29 r2-digital up up clearfwd idle y
0/2/0:1 30 r2-digital up up clearfwd idle y

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z:
Router(config)# controller E1 0/2/0
Router(config-controller)# ds0 busyout 21,29,30,24
Router(config-controller) # no ds0 busyout 21,29,30,24
Router(config-controller)# end
Router# show vo po sum | include clearfwd
Router# -->
```

- CSCtd90030

  Symptoms: A Cisco 2851 router may crash with a bus error.

  Conditions: The symptom is observed when the function calls involve Session Initiation Protocol (SIP) and it is possibly related to an IPCC server. It is seen with Cisco IOS Release 12.4(24)T1 or Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtd90367

  Symptoms: Router crashes every 2-3 days with URLF feature. The error message shows memory leak issues.

  Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(24)T2, with URLF features on the device.

  Workaround: There is no workaround.

- CSCtd98344

  Symptoms: NAT/PAT does not create more than one translation entry for all VRFs after a translation in the first VRF.

  Conditions: This symptom is observed when there is more than one VRF.

  Workaround: There is no workaround.

- CSCte27805

  Symptoms: Self ping on a dialer interface fails when it is over a PPPoE link.

  Conditions: The symptom is observed when the dialer interface is up and its underlying interface is PPPoE.

  Workaround: There is no workaround.

- CSCte27828

  Symptoms: Call forward does not work.

  Conditions:

  Topology:

  call originally is H323 then to CUCM---(SIP)---CUBE-- (SIP)---SIP Provider

  IP addresses:

  - CUCM 10.10.10.3
  - Cube SUD 10.10.10.2
  - CUBE North 192.168.101.10
  - SBC 192.168.100.5

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

  When the "call forward no answer" fails, we see a malformed contact field on 183 forwarded from CUBE to SBC (the same from CUCM to CUBE is correct); SBC does not answer due to this.

  Workaround: There is no workaround.

- CSCte30224

  Symptoms: A Cisco IOS device may unexpectedly restart when executing a Tcl script that has been compiled into bytecode.

  Conditions: This symptom is observed if the Tcl script tries to generate a random number using the **expr** *rand()* command.

  Workaround: Do not use the **expr** command to generate random numbers, or do not compile the Tcl script into bytecode.

- CSCte68795

  Symptoms: High CPU utilization is observed with IP NBAR protocol discovery.

  Conditions: The symptom is observed when enabling the **ip nbar protocol discovery** command.

  Workaround: Use the previous version of WINMX PDLM.

- CSCte76760

  Symptoms: A router acting as a voice gateway may unexpectedly reload due to bus error.

  Conditions: The symptom is observed when the gateway is experiencing a low memory problem leading to seeing SYS-2-MALLOCFAIL errors.

Workaround: Resolve the low memory problem.

- CSCte89130

  Symptoms: Router experiences a memory leak.

  Conditions: The router is running out of memory due to the CCSIP_SPI_CONTROL process (as shown by the **show mem alloc total** command).

  Workaround: There is no workaround.

- CSCte93792

  Symptoms: Virtual access bound to an ATM interface does not come up.

  Conditions: The symptom is observed when two ATM interfaces are part of multilink PPP by virtual access in dialer interface. The PVC of one of the ATM interfaces is removed and then re-added. The virtual access of the other ATM interface is affected and does not come up.

  Workaround: There is no workaround.

- CSCte98702

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

  Conditions: The symptom is observed when NAT is configured.

  Workaround: There is no workaround.

- CSCtf41721

  Symptoms: A DMVPNv6 hub might crash upon doing a shut/no-shut on the tunnel interface of the other hub.

  Conditions: The symptom is observed with the following steps:

  1. Configure DMVPNv6 with two hubs and two spokes.

  2. Hub 2 tunnel is shut and unshut.

  3. Hub 1 crashes.

  Workaround: There is no workaround.

- CSCtf51690

  Symptoms: Router crashes when a packet with out-of-bound featureIndex values is sent to the CME.

  Conditions: The symptom is observed when malformed packets are sent to the CME with out-of-bound featureIndex values in fStationFeatureStatReqMessage.

  Workaround: There is no workaround.

- CSCtg19546

  Symptoms: MPLS forwarding of labeled frames across a tunnel may fail. This symptom arises when an incorrect TAG adjacency is created for the tunnel.

  Conditions: This symptom is observed when adding or removing crypto and a tunnel protection configuration from a tunnel interface also configured with MPLS. When this symptom occurs, an incorrect or missing IPSec post encap feature is observed under the TAG adjacency for the tunnel.

  Workaround: Removing the crypto and/or removing and reconfiguring mpls ip from the tunnel can recover connectivity.

Alternate Workaround: VTI cannot be combined with MPLS label switching, since IPSec can only encapsulate IP packets, not MPLS packets. This is due to design. In GRE mode, however, this is possible, so use a GRE tunnel with IPSec tunnel protection along with MPLS label switching. Be sure to remove and reapply the "tunnel protection ipsec profile" configuration so that IPSec features will be properly applied to the IP-and MPLS-switching feature paths.

- CSCtg46715

  Symptoms: A PPP PE call fails with multilink enabled on a group async/dialer interface. During the IPCP phase, the "PPPoX: Error in dialer_profile_pppox_oqueue" message appears.

  Conditions: This symptom occurs when multilink is configured and when "multilink" code binds a Vaccess interface for the bundle to the same profile as the first link.

  Workaround: There is no workaround.

- CSCtg67346

  Symptoms: After some time of normal operation, a dialer interface (dialer profile configuration) might become stuck. Debugs would only show "Di1 DDR: dialer_fsm_pending() di1".

  Conditions: The conditions are unknown at this time.

  Workaround: Remove the affected dialer and put the configuration on another dialer.

- CSCth11006

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCth38699

  Symptoms: Cisco IOS platforms configured for Auto-RP in a multicast environment lose the RP-to-group mappings.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(18)SXF7, Release 12.2(33)SXH4, and Release 12.2(33)SRC4, but it is believed to affect other releases. This symptom occurs when the length of the RP-Discovery packet reaches its limit. If the Mapping Agent receives RP-Announce packets, increasing the number of multicast groups, and that number makes the limit of the packet size, then an empty RP-Discovery packet is triggered that clears the RP-to-Group mapping tables in all the routers receiving such a packet.

  Workaround: Configure static RP-to-Group mappings.

- CSCth48457

  Symptoms: A crash is seen at qos_classify_opttype.

  Conditions: The symptom is observed when changes are being made to the service policy while traffic is running. It is seen when using the same child policy-map in multiple classes of the parent and then removing the child policy-map by unconfiguring the parent classes. It happens with the following Cisco IOS Releases: 12.4(15)T, 12.4(20)T, 12.4(22)T, 12.4(24)T, 15.0(1)M, and 15.1(1)T.

Workaround 1: Define the policy-map you wish to run before applying it on the interface level.

Workaround 2: Do not use the same child policy in multiple classes of the parent.

- CSCth52720

  Symptoms: With client-initiated L2TPv2, IPCP packets are not sent when MLP is enabled.

  Conditions: The symptom is observed when PPP multilink is configured with Cisco IOS Releases 12.4(24)T3, 12.4(11)XJ, and 15.1(1)T.

  Workaround: Remove the PPP multilink configuration or use Cisco IOS Release 12.3(14)T6.

- CSCth75435

  Symptom: When the pak->particulequeue.count = 0 is executed, at that time the pak structure have no particle. So the head and tail pointer associated with the pak data structure should be set to NULL. This is not the case and due to this when the static pak structure is used for the next time it already has some stray pointer.

  Condition: When the pak->particulequeue.count = 0 is set the head and tail pointer associated with pak should also be set to NULL.

  Workaround: There is no workaround.

- CSCth80642

  Symptoms: Cisco IOS SSLVPN fails to accept new SSL connection. Sessions get stuck in Time Wait until TCP queue is full.

  Conditions: SSLVPN on Cisco IOS.

  Workaround: The **clear tcp tcb** * command will clear Time Wait sessions.

- CSCti10928

  Symptoms: Xcoder sends empty RTP stream in one direction only.

  Conditions: The symptom is observed on a CUBE that is running Cisco IOS Release 12.(24)T3 with an incoming fast start call.

  Workaround: There is no workaround.

- CSCti13493

  Symptoms: A router crashes and the following traceback is seen:

  ```
  ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
  ASSERTION FAILED : ../voip/ccvtsp/vtsp.c: vtsp_cdb_assert: 1491: unkn - Traceback=
  %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 47523D58. - Process= "DSMP",
  ipl= 0, pid= 226, -Traceback=
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x430853EC
  ```

  Conditions: The symptom is observed with the DSMP process.

  Workaround: There is no workaround.

- CSCti48483

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

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

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

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at

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

- CSCti48504

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

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

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

- CSCti66454

  Symptoms: Router crashes when using the **show crypto session detail** command after using the **clear crypto session** command.

  Conditions: This symptom is observed when the router is running any form of tunnel protection, and SAs have been cleared. Then the user executes a **show** command.

  Workaround: Wait a few moments (30 seconds) between the **show** command and the **clear** command.

- CSCtj03381

  Symptoms: NAT traffic is getting process switched when you configure “nat entry” or you reload the router.

  Conditions: The symptom is observed when you enable VRF-aware NAT with the “match-in-vrf” option.

  Workaround 1: Reconfigure “ip cef”.

  Workaround 2: Do a **clear ip route vrf <vrf> ***.

- CSCtj20545

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

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

  Workaround: Shorten the keepalive timeout on the other endpoint.

- CSCtj21045

  Symptoms: Header compression decodes RTP timestamp incorrectly.

  Conditions: This issue occurs mainly with IPHC format compression interacting with older Cisco IOS releases.

  Workaround: Use IETF format compression.

- CSCtj46670

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

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

  Workaround: Reload the router.

- CSCtj47696

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

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

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

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

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

- CSCtj47829

  Symptoms: A buffer leak is experienced with “traffic-export” configured.

  Conditions: The issue seen when you export traffic to an interface and to an NME-APPRE-502-K9. All conditions are not completely known yet.

  Workaround: Disable the traffic-export functionality, for example:

  Traffic Export Configurations

  ```
  ip traffic-export profile axp-netscout
  interface Integrated-Service-Engine1/0
  bidirectional
  mac-address 0080.8c00.0001

  interface FastEthernet0/0.99
  encapsulation dot1Q 99
  ip address xxx.xxx.xxx.xxx 255.255.255.0
  ip traffic-export apply axp-netscout
  ```

  Remove the Configurations

  ```
  interface fa0/0.99
  no ip traffic-export apply axp-netscout
  no ip traffic-export profile axp-netscout
  ```

- CSCtj77285

  Symptoms: Router CPU becomes high tending towards 80%+ from normal operating conditions. The command **show mem | inc FNF OCE** will show multiple rows rather than just a couple of rows.

  Conditions: The symptom is observed with voice calls and VOIP in use. It is seen when Flexible NetFlow is configured.

  Workaround: Switch off Flexible NetFlow (although that leaves memory consumption in place and CPU higher than normal) or reboot the router.

- CSCtk34885

  Symptoms: Crosstalk being heard intermittently on inbound calls.

Conditions: Inbound calls from PSTN to Ingress gateway hearing crosstalk on Rout call leg (DSP to PSTN) on AS5400XM.

Workaround: The following command in IOS can mitigate this for SIP:

voice service voip sip source filter

This eliminates the risk for crosstalk since the gateway blocks all rogue audio out to the PSTN with this command.

The above command only works for SIP, so H323, MGCP, and SCCP are still affected.

The following enhancement requests have been filed:

- CSCtq47019: Support on H.323, SCCP, and MGCP. This will allow the command to be used in all VoIP environments.
- CSCtq47431: To get this feature added to IP phones.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 1.8/1.6:

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

No CVE ID has been assigned to this issue.

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

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

- CSCtk53674

  Symptoms: A router that is running Cisco IOS Release 12.4(15)T14 and Cisco IOS Release 15.0M will crash when the SNMP v3 configuration is removed.

  Conditions: This symptom occurs when the running configuration contains the following depending on the Cisco IOS release:

  Cisco IOS Release 12.4(15)T14

  ```
  snmp-server user QOSqosuser1 QOSqosgroup v3 enc auth sha <DIGEST>
  priv aes 128 qosQOO!priv acc SNMP
  ```

  Cisco IOS Release 15.0(1)M4

  ```
  snmp-server user QOSqosuser1 QOSqosgroup v3 enc auth sha <DIGEST>
  priv aes 128 qosQOO!priv acc SNMP
  ```

  When you remove the above configuration using the **no snmp-server user** command, the router crashes.

  Workaround: There is no workaround.

- CSCtk54830

  Symptoms: An ARP entry is removed from the ARP table by DHCP.

  Conditions: This symptoms happens while replying to the client Request/Inform.

  Workaround: There is no workaround.

- CSCtk55107

  Symptoms: A router crashes due to SIP.

  Conditions: This symptom is observed when SIP is configured.

  Workaround: The only workaround is to disable SIP.

- CSCtk65429

  Symptoms: In an encrypted CE-PE session, traffic sourced by the VRF (for example, ping) works, but traffic coming from MPLS does not reach the crypto map.

  Conditions: This issue is observed in CEF code images, like Cisco IOS Release 12.4(22)T2, 12.4(24)T4, and 15.1(3)T. This issue is not observed in 12.4 mainline releases, such as Cisco IOS Release 12.4(25d).

  Workaround: There is no workaround.

- CSCtk67934

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

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

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

- CSCtl05684

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

  Conditions:

  - This symptom is observed when running EzVPN and if Xauth is performed by different username during P1 rekey.
  - Use NAT in the VPN path.

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

- CSCtl54975

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

  Conditions: Unknown.

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

- CSCtl73914

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

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

  Workaround: There is no workaround.

- CSCtl90341

  Symptoms: A router crashes due to an NHRP stack overflow.

  Conditions: This symptom occurs very inconsistently.

  Workaround: There is no workaround.

- CSCtn00405

  Symptoms: A Cisco router may crash when “isdn test call” is run.

Conditions: This symptom has been experienced on multiple IOS versions, including Cisco IOS Release 12.4(15)10, 12.4(24)T4, and 15.0(1)M4.

Workaround: There is no workaround.

- CSCtn08208

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

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

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

- CSCtn19496

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

  ```
  Scheduler_flags 177
  ```

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

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

  Workaround: There is no workaround.

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

- CSCtn31333

  Symptoms: CPU utilization is high due to the process Net Background.

  Conditions: This symptom is observed on a router used for LNS with an L2TP application after upgrading to Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCtn65060

  Symptoms: A Cisco device crashes.

  Conditions: This symptom is observed with Cisco IOS Release 15.0M and Release 15.1T when configuring “snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL.”

  Workaround: Avoid using the **snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL** command.

- CSCtn65655

  Symptoms: The applied QoS policy is not seen, after it is removed from the PVC and re-applied.

  Conditions: Both the input policy and the output policy must be applied. The issue was not seen with only one policy applied in the lab.

  1. Both service policies are applied to the OUT and IN directions on the ATM PVC.

  2. Remove the service policy applied to the OUT direction.

  3. Exit from ATM PVC mode, enter ATM PVC mode again, and confirm that the policy is removed.

  4. Re-apply the service policy and exit.

  5. The OUTBOUND policy is not applied (nothing shows up in “show policy-map int <target> out”) though upon “show run” the configuration is seen.

  Workarounds:

Workaround #1: Perform a shut/no shut on the PVC in order for the policy map to be applied correctly.

Workaround #2: (Affects both inbound and outbound policies):

1. Remove both the input and output service policies from the PVC.

2. Exit configuration mode.

3. Make necessary changes to policy maps (for example, policing rates, WRED thresholds).

4. Re-add both the input and output service polices to the PVC.

5. Exit configuration mode.

Workaround 3#: (Affects only the outbound policy):

1. Remove the output service policies from the PVC.

2. Add the “junk” outbound service policy to the PVC.

3. Exit configuration mode.

4. Make necessary changes to policy maps (for example, policing rates, WRED thresholds).

5. Remove the outbound “junk” service policy from the PVC.

6. Re-add the original outbound service policy to the PVC.

7. Exit configuration mode.

- CSCtn74169

  Symptoms: Crash by memory corruption occurs in the “EzVPN Web-intercept daemon” process.

  Conditions: This symptom is observed when EzVPN server pushes a long banner to the client after HTTP authentication using HTTP intercept.

  Workaround: Do not use long banner in HTTP intercept.

- CSCtn77090

  Symptoms: Gradual increase of CPU with CPU topping at 99% and increase in holding memory for IP SLA process may cause crash on routers that are running IP SLA probes, generally above 300 probes.

  Conditions: This symptom is observed when there are more than 20 SNMP simultaneous probe restarts from IP SLA management software.

  Workaround: Limit SNMP probe restarts to under 20 from IP SLA management software.

- CSCtn77154

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

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

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

- CSCtn87012

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

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

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

- CSCto08135

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

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

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

- CSCto08754

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

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

  Workaround: There is no workaround.

- CSCto60047

  Symptoms: A crash occurs either due to a chunk corruption or at ssh_send_queue_data.

  Conditions: This symptom occurs under the following conditions:

  - An SSH session exists between two routers.
  - The **show tech** command is issued and then aborted.

  Workaround: There is no workaround.

- CSCto63954

  Symptoms: A router with GETVPN configurations is continuously crashing.

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

  Workaround: There is no workaround.

- CSCto88686

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

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

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

- CSCtq05004

  Symptoms: A dialer loses its IP address sporadically.

  - "show interface atm x" will record output drops during the issue:

    ```
    ATM0 is up, line protocol is up
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 31956 <<
    Incrementing during the issue
    ```

  - "show interface queueing atm0.1" (hidden command) will show as follows:

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

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

```
PPP: Missed 5 keepalives, taking LCP do\wn PPP DISC: Missed too many keepalives
```

  - There will be no ATM (physical interface) flap in this case (during the issue).
  - A shut/no shut on the ATM interface does not help.

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

  Workaround: Reload.

- CSCtq05636

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

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

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

  In Cisco IOS Release 15.1(3)T1, the * character is not forwarded.

  Conditions: This symptom is observed when CUBE performs SIP to SIP interworking. This issue is seen only with Cisco IOS Release 15.1(3)T1.

  Workaround: Upgrade the code to Cisco IOS Release 15.1(3)T or Cisco IOS Release 15.1(M4).

- CSCtq07413

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

  Conditions: This symptom is observed in Cisco IOS Release 12.4(15)T6.

  Workaround: Use software encryption.

- CSCtq09899

  Symptoms: The VXML gateway crashes.

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

  Workaround: There is no workaround.

- CSCtq10684

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

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

  Workaround: A possible workaround is to reload the box.

- CSCtq63625

  Symptoms: WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4 is not getting trained with some DSLAMs without "line rate" configured manually. It gets trained with a manual line rate configured.

  Conditions: WIC-1SHDSL-V3 with Cisco IOS Release 12.4(24)T4.

  Workaround: There is no workaround.

- CSCtq86500

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

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

  Workaround: Disable VSA and use software encryption.

- CSCtq92940

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

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

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

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

- CSCtr07142

  Symptoms: A memory leak is seen at crypto_ss_open.

  Conditions: No special configuration is needed.

  Workaround: There is no workaround.

  Further Problem Description: At bootup, when the **show memory debug leaks** command is run, memory leak entries are seen for the crypto_ss_open process.

- CSCtr15891

  Symptoms: On-demand DPD is being sent on every IPsec SA even though a response is seen on at least one of them.

  Conditions: Periodic DPD is configured, and multiple IPsec SAs exist with the peer with outbound traffic flowing on each of them without any inbound traffic.

  Workaround: There is no workaround.

- CSCtr49064

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

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

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

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

- CSCtr84800

  Symptoms: An accounting stop is not triggered from DHCP when a client releases the binding.

  Conditions: A DHCP server has a pool with accounting set. When a DHCP client releases the lease, an accounting stop is not sent.

  Workaround: There is now workaround.

Resolved Caveats—Cisco IOS Release 12.4(24)T5

Cisco IOS Release 12.4(24)T5 is a rebuild release for Cisco IOS Release 12.4(24)T. The caveats in this section are resolved in Cisco IOS Release 12.4(24)T5 but may be open in previous Cisco IOS releases.

- CSCsv66694

  Symptoms: If the router has a static route and that route is redistributed into EIGRP with a route-map, the EIGRP topology table shows that the router is setting the tag on the redistributed route. However, both the routing table and the EIGRP topology table do not show the tag as being set.

  Conditions: This symptom is observed when a Cisco ASR 1006 router that is running Cisco IOS Release 12.2(33)XNB1 is EIGRP neighbors with a Cisco 7300 series router (running Cisco IOS Release 12.2(31)SB10).

  Workaround: There is no workaround.

- CSCsv97424

  Symptoms: A router will reload due to memory corruption in the I/O pool. As an indication for this bug, we will see the same caller PC in the output of the show buffer pool Serial0/0/0 command.

  Conditions: This symptom is observed on Cisco routers that are running the adventerprisek9_ivs-mz feature set and when packets are being processed by an ATM interface.

  Frequency: Always.

  Workaround: We can overcome the reload issue by disabling hardware crypto using the following command in global configuration mode: “no crypto engine accelerator”.

  Note When the hardware crypto is turned off, encryption and decryption will be done by software and not by hardware. This can slightly hike CPU utilization. But, this should not be an issue as long as huge volume of traffic does not exist.

- CSCsw38009

  Symptoms: Packet drops are seen on an ATM interface when it is used as a tunnel source.

  Conditions: This symptom is observed as soon as **Per SA QoS** is configured on the tunnel interface.

  Workaround: This symptom is not observed on Ethernet.

- 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 commands **show tech** or **show as5400** are executed.

  Workaround: There is no workaround.

- CSCta07805

  Symptoms: Chunk corruption crashes with FW. The following error may be

  observed:

  ```
  %SYS-2-CHUNKBADREFCOUNT: Bad chunk reference count
  ...
  -Process= “FW DP Inspect process”
  ```

  Conditions: This symptom occurs when FW is configured on the box.

Workaround: There is no workaround.

- CSCta11223

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

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

  Workaround: There is no known workaround.

- CSCta38476

  Symptoms: When removing the tunnel interface with CDP enabled, tracebacks are generated. CDP does not come up in all the interfaces.

  Conditions: This symptom is observed with large numbers of CDP neighbors in an MCP router.

  Workaround: Disable CDP before deleting the tunnel interface.

  Further Problem Description: CDP tries to send a packet over a deleted tunnel interface causing the issue.

- CSCta95295

  Symptoms: A Cisco router terminates 100+ VPN tunnels when using CRL checking for the Phase 1 authentication.

  Conditions: If IKE gets stuck for any reason, it might cause IOMEM to be depleted completely, which could lead to a router crash.

  Workaround: Disable CRL checking or use pre-shared keys.

- CSCta98976

  Symptoms: A Cisco IOS certificate server (CS) may crash during a CA certificate rollover.

  Conditions: This symptom is observed with similarly-named keys.

  Workaround: Rename similarly-named keys. For example, the keys named SubCA are a subset of the SSH keys named SubCA.server. Rename the SSH keys using the **ip ssh rsa keypair-name** command.

- CSCtb17152

  Symptoms: A large packet drop may occur when FRF.12 is enabled.

  Conditions: This symptom is observed when FRF.12 is enabled.

  Workaround: There is no workaround.

- CSCtc06935

  Symptoms: Packet loss occurs between two Cisco 3200 MAR routers connected over FESMIC Fast Ethernet ports via wireless radios, after upgrading to Cisco IOS Release 12.4(22)T2.

  Conditions: The symptom is observed with the following conditions:

  - After a code upgrade.
  - On Cisco 3200s connected via wireless radios.

  It does not occur on devices directly connected via fiber.

  Workaround: Use Cisco IOS Release 12.4(1a).

- CSCtc65347

  Symptoms: A Cisco 3845 may have a processor pool memory leak in the SNMP Engine.

  Conditions: This symptom is observed on a Cisco 3845 running Cisco IOS Release 12.4(20)T1 and polling specific VoIP MIBs.

  Workaround: Do not poll VoIP Peer CFG Entry MIBs or use an SNMP view to block the router from replying to the said poll, such as:

  ```
  snmp-server view leak internet included
  snmp-server view leak cvVoIPPeerCfgEntry excluded
  snmp-server community <community name> view leak
  ```

  Further Problem Description: "Show proc mem <pid>" (where <pid> is the process id for the SNMP ENGINE) should decode to VoIP Peer Cfg Entry mibs being polled.

- CSCtd10712

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCtd39579

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

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

  Workaround:

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

- CSCtd74943

  Symptoms: Multiple PPPoE clients cannot be configured on a single ATM VC.

  Conditions: This symptom is observed under all conditions.

  Workaround: There is no workaround.

- CSCtd87788

  Symptom: Traceback is seen when serial from second CJ-PA controller is added and removed from multilink. This interface remains up/down until a reload.

  Conditions: This symptom is seen when serial from second controller in unchannelized mode is added to multilink.

  Workaround: Reload the box to bring up the interface.

- CSCte50870

  Symptoms: A Cisco AS5400 router crashes due to a watchdog timeout. CPU hogs due to the “SERIAL A’detect” process are seen before the reload:

  ```
  %SYS-3-CPUHOG: Task is running for (36000)msecs, more than (2000)msecs (36/6),process
  = SERIAL A’detect.
  ```

  After some time the device crashes:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SERIAL A’detect.
  ```

  Conditions: The symptom is seen on a Cisco AS5400 router that is running Cisco IOS Release 12.4(24)T2. The serial interfaces of the device are configured with “autodetect encapsulation xxx” and router system clock has been updated:

  ```
  %SYS-6-CLOCKUPDATE: System clock has been updated from 10:42:09 UTC Wed May 19 2010 to
  11:42:09 MET Wed May 19 2010, configured from console by console. %SYS-6-CLOCKUPDATE:
  System clock has been updated from 11:42:09 MET Wed May 19 2010 to 12:42:09 MET-DST
  Wed May 19 2010, configured from console by console.
  ```

  Workaround: If possible, remove this command.

- CSCtf56107

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

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

  Workaround: There is no workaround.

- CSCtf77047

  Symptoms: Ping ATM subinterface peer IP address has packet loss from Cisco 7206.

  Conditions: This symptom occurs with the following:

  1. NPE-G2+PA-MC-STM-1SMI+PA-A6-OC3SML
  2. Enable EIGRP on ATM subinterface

  Workaround: There is no workaround.

- CSCtf80105

  Symptoms: When basic SIP-SIP calls are placed using automation scripts, calls start failing due to UDP socket connection error

  Conditions: The symptom is observed when the router is configured with a dial peer and with SNMP. A dial peer is most likely required to reproduce the issue, but it is possible that a different UDP protocol other than SNMP could also cause the symptom. Once a call failure occurs, all the calls placed later will fail with a UDP socket connection error.

  Workaround: Use the following steps:

  1. Under sip-ua, configure “connection-reuse” (which is a hidden command).
  2. Configure the use of TCP.

- CSCtf99622

  Symptoms: Web Cache Communications Protocol (WCCP) Generic Routing Encapsulation (GRE) returned packet gets dropped on Cisco 7200 series routers, when the interface has multiple subinterfaces configured in more than one routing domain and is passing SSL/HTTPS traffic.

Conditions: This symptom occurs when multiple subinterfaces are present on the same physical interface, out of which one subinterface is management and the other subinterfaces are for traffic. The GRE-returned packet from the Wide-Area Application Engine (WAE) uses the wrong subinterface (mgmt instead of traffic) to route packet and hence the packet gets dropped and no throughput is seen.

Workaround 1: Use IP Routing Table Manager (RTM) instead of configuring WAE with GRE Routing Transit Number (RTN).

Workaround 2: Use physical interfaces on the Cisco 7200 platform instead of subinterfaces.

- CSCtg14446

  Symptoms: Packets are dropped in excess of the configured rate for hierarchical policies, with shaper in the parent policy.

  Conditions: The symptom is observed only with HQoS policies (flat policies are not affected).

  Workaround: There is no workaround.

- CSCth03022

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

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

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

- CSCth04193

  Symptoms: A Cisco router crashes at **cce_dp_named_db_http_free_token_info**.

  Conditions: This symptom is observed when Zone-based Policy Firewall is configured to inspect HTTP traffic.

  Workaround: Do not use deep packet inspection.

- CSCth15268

  Symptoms: Cisco IOS stops forwarding LLC I frames but continues to respond to poll frames. Finally, Cisco IOS might disconnect the LLC session.

  Conditions: This symptom can happen if the remote client drops an LLC packet with the poll bit ON.

  Workaround: Set “llc2 local-window” to 1.

- CSCth16382

  Symptoms: A Cisco device crashes at **cce_dp_results_get_class_group_element**.

  Conditions: This symptom is observed when Crypto is on and QoS pre-classify is not enabled. The crash occurs when configurations are loaded and traffic is run.

  Workaround: There is no workaround.

- CSCth18146

  Symptoms: A Cisco SIP gateway may reload unexpectedly due to a release message with no IEs.

  Conditions: This symptom is observed on a SIP gateway with tunneling enabled.

Workaround: There is no workaround.

- CSCth20696

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

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

  Workaround: There is no workaround.

- CSCth26441

  Symptoms: Non-broadcast Ethernet frames are dropped by the GigabitEthernet1/0 controller that connects to the NME module.

  Conditions: This symptom is observed when xconnect is configured on a subinterface and 802.1q trunking is used to connect to the NME module.

  Workaround: There is no workaround.

- CSCth58283

  Symptoms: NAT/CCE interoperability can cause a crash and several other issues.

  Conditions: This symptom occurs when NAT is enabled.

  Workaround: There is no workaround.

- CSCth62136

  Symptoms: The ISDN L2 goes to "Layer 2 NOT Activated."

  Conditions: This symptom is observed when a service policy is attached to the dialer interface.

  Workaround: Remove the service policy from the interface.

  Further Problem Description: This symptom is not seen with the following Cisco IOS Releases:

  - 12.4(13d)
  - 12.4(15)T12

  This symptom is seen with the following Cisco IOS Releases:

  - 12.4(22)T5
  - 12.4(24)T3
  - 15.0(1)M3

- CSCth68038

  Symptoms: After a simulated failover of an L2L tunnel, a Cisco 7200 series router with VSA, fails to encrypt traffic for a period of time, typically for several minutes. VSA then begins to encrypt traffic correctly.

  Conditions: The problem appears to be triggered when manually failing over a spoke from one hub Cisco 7200 (without VSA) to a secondary hub Cisco 7200 with VSA. The issue only affects virtual-template interfaces.

  Workaround: Use software encryption.

- CSCth69364

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCth70437

  Symptoms: Crypto sessions drop after the following error message:

  ```
  000059: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
  ptr=83D91910, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
  0x8039460Cz 0x80397B40z
  000060: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
  ptr=83D91CE4, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
  0x8039460Cz 0x80397B40z
  000061: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
  ptr=83D920B8, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
  0x8039460Cz 0x80397B40z
  000062: *Jul  1 14:01:31 DST: %SYS-2-BADSHARE: Bad refcount in datagram_done,
  ptr=83D82F8C, count=0,  -Traceback= 0x80334D4Cz 0x823409A0z 0x8230D830z
  0x8039460Cz 0x80397B40z
  ```

  Conditions: This symptom is observed on Cisco IOS 800 series routers and when crypto is applied to dialer interface.

  Workaround: There is no workaround.

- CSCti03808

  Symptoms: A Cisco 7200 series router may crash with a fatal error.

  Conditions: This symptom is observed only when PA-POS-1OC3 and C7200-VSA port adapters are installed and the encrypted traffic is being sent through the POS interface. The problem is more likely as traffic load increases.

  Workaround: Use a different POS port adapter or VAM module instead of the VSA encryption module.

  Further problem description: During investigation, the router occasionally hangs instead of crashing. With the fix for this symptom the hangs are not observed.

- CSCti07805

  Symptoms: Router reloads @sipSPIUpdSrtpSession.

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

  Workaround: There is no workaround.

- CSCti22544

  Symptoms: IKE fails to come up while using RSA signature. PKI debugs show the following message:

  ```
  PKI-4-CRL_LDAP_QUERY: An attempt to retrieve the CRL from
  ldap://yni-u10.cisco.com/CN=nsca-r1 Cert Manager,O=cisco.com using LDAP has failed
  ```

  Conditions: This symptom is observed when the VRF-aware IPsec feature is used and VRF-label is configured under trustpoint. For example:

  ```
  crypto pki trustpoint yni-u10 enrollment url http://yni-u10:80 vrf coke
  ```

  Workaround: There is no workaround.

- CSCti23087

  Symptoms: “Protocol not in this image” message is displayed while configuring EIGRP.

  Conditions: This symptom occurs while configuring EIGRP.

Workaround: There is no Workaround.

- CSCti25339

  Symptoms: A Cisco IOS device may experience a device reload.

  Conditions: This symptom occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  Workaround: There is no workaround.

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

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

  CVE ID CVE-2010-3050 has been assigned to document this issue.

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

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

- CSCti54173

  Symptoms: A leak of 164 bytes of memory for every packet that is fragmented at high CPU, is seen sometime after having leaked all the processor memory. This causes the router to reload.

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

  Workaround: There is no workaround.

- CSCti62801

  Symptoms: When both Caller-ID (CID) and Call-Waiting (CW) features are enabled on SIP analog endpoint, repetitive Call-Waiting (CW) tone is not played every 10 seconds until call is answered.

  Conditions: The symptom is observed with a SIP analog endpoint on IAD243x, when the Device Service Application (DSAPP) is enabled on the gateway to provide supplementary features using SIP for the phone connected to the FXS port.

  Workaround: There is no workaround.

- CSCti66153

  Symptoms: A Cisco 7200 series router with VSA in GETVPN deployment logs the following error:

  ```
  %VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption error, Selector checks.
  ```

  Conditions: The following conditions need to be met:

  - A Cisco 7200 series router with VSA in receive-only mode.
  - Keyserver in receive-only mode. - Other GM in passive mode (that is encrypting outbound traffic) sending traffic to the "inside" of the Cisco 7200.
  - Traffic matching a keyserver delivered crypto ACL matching L4 ports (for example: **permit tcp any any eq 23**).

  Workaround: Relaxing any of the conditions here above:

  1. Use VAM2+ instead of VSA.
  2. Use GETVPN ACL without l4 ports (For example.: **permit ip any any**).
  3. Have the Cisco 7200 in passive mode as well.
  4. Not using receive-only mode on the keyserver.

- CSCti77879

  Symptoms: When the traffic to encrypt matches the first sequence of a crypto map, starting its crypto ACL with a deny statement, the traffic is dropped whether or not this deny statement is a subset of the permits contained in that crypto ACL or not.

  Also, the limitation of 14 denies in an ACL due to the jump behavior does not seem to be present.

  Conditions: The symptom is observed in a VSA installed in a Cisco 7200 series router that is running Cisco IOS Release 15.0(1)M3.

  Workaround: There is no workaround.

  Further Problem Description: As the configuration guide states, the **crypto ipsec ipv4-deny {jump | clear | drop}** command should help to avoid this problem, but this command is not available for the VSA, only for VPN SPA.

- CSCti90602

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

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

  Workaround: There is no workaround.

- CSCti98219

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCti99419

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

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

  Workaround: Power-cycle the router.

- CSCtj07885

  Symptoms: A Cisco router may unexpectedly reload due to a bus error during an SNMP poll for the **ccmeActiveStats** MIB.

  Conditions: The router may crash when it is configured as SRST (call-manager-fallback) or CME-as-SRST with "srst mode auto-provision none", when interworking with SNMP, using the MIB browser query **ccmeActiveStats**.

  Workaround:

  1. Configure CME-as-SRST with "srst mode auto-provision all".
  2. Stop the ccmeActiveStats MIB from being polled on the router. There are three possible ways to do this:

a. Stop the MIB on the NMS device that is doing the polling.

b. Turn off SNMP polling on the device.

c. Create a view to block the MIB and apply it to all SNMP communities.

- CSCtj09256

  Symptoms: AnyConnect client fails to connect. The following error messages may be seen:

  ```
  Unable to Process Response from server <servername or IP address of gateway>
  Connection attempt has failed due to server communication errors. Please retry the
  connection
  ```

  Conditions: The symptom is observed on a Cisco router that is running Cisco IOS Release 12.4(24)T4.

  Workaround 1: Use the clientless portal to launch AnyConnect.

  Workaround 2: Use Cisco IOS Release 12.4(24)T3 or earlier.

- CSCtj41194

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

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

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

- CSCtj66392

  Symptoms: Tunnel interface does not go up on standby router and IKE and IPSec SAs are not synchronized to the standby router. Even if tunnel protection is configured, crypto socket is not opened.

  Conditions: This symptom is observed when IPSec stateful failover for tunnel protection is configured.

  Workaround: Use Cisco IOS Release 12.4(11)T4.

- CSCtj81533

  Symptoms: The following error messages is seen:

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

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

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

  Workaround: There is no workaround.

- CSCtj86514

  Symptoms: An SNMP walk on Cisco AAL5 MIB may not return information for all PVCs configured on the device.

  Conditions: An SNMP walk query on the Cisco AAL5 MIB may fail to return information of bundled PVCs that are in down state. Information about PVCs in UP state is returned correctly.

Workaround: To get information of bundled PVCs in down state, you need to poll with more specific OIDs. Instead of doing an snmpwalk on "**1.3.6.1.4.1.9.9.66.1.1.1.1.3**", do an snmpget on "**1.3.6.1.4.1.9.9.66.1.1.1.1.3.<IfIndex>.<VPI>.<VCI>**".

- CSCtj87180

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

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

  Workaround: There is no workaround.

- CSCtj96915

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

  Conditions: Unknown. See Further Problem Description below.

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

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

- CSCtk15123

  Symptoms: BGP routes are not sent to the EBGP peer.

  Conditions: This symptom is observed with neighbor x.x.x.x advertise-map .. exist-map .. This issue is timing-related and is not very easy to reproduce.

  Workaround: "Clear ip bgp x.x.x.x soft out" can be done to advertise the routes.

- CSCtk56570

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

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

  Workaround: Disable media transcoder-high-density.

- CSCtk60909

  Symptoms: Router crashes due to interrupt stack low.

  Conditions: This symptom occurs when the router is as SWMTP and makes more than 6 transfer calls.

  Workaround: There is no workaround.

- CSCtk74685

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

  Observed with "debug cch323 all" and "debug ip tcp trans":

```
13090333: Dec  3 13:18:20.965: //137091/80C6B1F78F31/H323/run_h245_iwf_sm:
received IWF_EV_H245_DISCONN while at state IWF_ACTIVE
```

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

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

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

Workaround: Use one of the following workarounds:

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

```
voice service voip h323 call preserve
System > Service Parameters > (Select Publisher Node) > Cisco CallManager > Advanced >
Allow Peer to Preserve H.323 Calls > False > Save
```

2. Run a Cisco IOS release that does not have the fix for CSCin76666.
3. Change the signaling protocol to SIP.

- CSCtk95992

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

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

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

  Further Problem Description: This symptom occurs in the following (and later) Cisco IOS Releases:

  - 12.4(15)T14
  - 12.4(24)T4
  - 15.0(1)M3
  - 15.1(1)S
  - 15.1(2)T
  - 12.2(33)SXI4
  - 12.2(33)SXI4a

- CSCtl20509

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

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

  Workaround: Reload the router.

- CSCtl21695

  Symptoms: An LNS configured for PPTP aggregation might stop accepting new PPTP connections after PPTP tunnels exceed one million.

  Debug vpdn l2x ev/er shows:

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

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

  Workaround: Reload LNS.

- CSCtl87879

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

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

  Workaround: There is no workaround.

- CSCtl92014

  Symptoms: After a reprompt element, “enumerate”, using internal variables like “_prompt” or “_dmtf”, no longer produce a valid list of options and repeat the last option.

  Conditions: This symptom occurs when running Cisco IOS Release 12.4(15)T and later releases.

  Workaround: There is no workaround.

- CSCtn22523

  Symptoms: IPSLA udp-jitter probes may crash at saaAddSeqnoDupQ in Cisco IOS Release 12.4T/15.0M. There is no impact to other releases.

  Conditions: This symptom is observed when the network experiences delay, and reordered and duplicate packets can trigger this problem when IPSLA udp-jitter is scheduled.

  Workaround: Disable udp-jitter probes.

Resolved Caveats—Cisco IOS Release 12.4(24)T4

Cisco IOS Release 12.4(24)T4 is a rebuild release for Cisco IOS Release 12.4(24)T. The caveats in this section are resolved in Cisco IOS Release 12.4(24)T4 but may be open in previous Cisco IOS releases.

- CSCee93607

  Symptoms: A VPN client cannot connect to a router that functions as an EzVPN server.

  Conditions: This symptom is observed on a Cisco router that functions as an EzVPN server when the user name is not sent in the RADIUS authentication request for the VPN client, causing the authentication server to reject the VPN client.

  Workaround: If this is an option, use local authentication.

  Further Problem Description: The following error message appears in the debug output:

  ```
  ISAKMP (0:1): FSM action returned error: 4
  ```

- CSCsk55161

  Symptoms: Cisco IOS software crashes when enabling multicast feature of scaled-up config.

Conditions: This symptom is observed under the following conditions:

  - More than 4000 VLANs are configured on a Port Channel.
  - All VLANs have a V6 configuration, and multicast is enabled on each of them at once.

Workaround: There is no workaround.

- CSCsk83505

  Symptoms: Under various circumstances, UDP input queues can grow to much larger than their intended size. This can result in memory allocation errors if the application that services a UDP input queue is unable to do so quick enough to keep up with incoming traffic. UDP needs to drop received packets, once a given input queue has reached its limit.

  Conditions: This symptom is observed with RIPv6 with a large number of neighbors in both Cisco IOS and ION images.

  Workaround: There is no workaround.

  Further Problem Description: The root cause is that several pieces of code are enqueuing packets to ipsocktype inq without checking its size, and without updating statistics.

- CSCsl64247

  Symptoms: Router crashes 20-30 minutes after configuring “mode route control”.

  Conditions: The symptom is observed when the router is configured as OER master.

  Workaround: There is no workaround.

- CSCso02147

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- 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.

- CSCsu31853

  Symptoms: TCP sessions in TIMEWAIT state cause buffer usage until they move to CLOSED state.

  Conditions: This symptom is observed with almost all TCP applications. It is mainly seen on low end switches.

  Workaround: There is no workaround.

- 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.

- CSCsx08019

  Symptoms: A crash may occur if a trustpoint is removed from a server at the same time as the server is trying to autoenroll.

  Conditions: This symptom is observed when the **no crypto pki trustpoint** *trustpointname* command is issued just as the autoenroll timer goes off.

  Workaround: Do not delete a trustpoint that is about to autoenroll. Either wait until it finishes, or turn autoenroll off before deleting the trustpoint.

- CSCsx14637

  Symptoms: Modem pass-through calls failing while handshaking

  Conditions: Problem appeared after upgrade from Cisco IOS Release 12.3(26) to Cisco IOS Release 12.4(23).

  Workaround: There is no workaround.

- CSCsx46383

  Symptoms: A Cisco Catalyst 6000 series switch does not respond with any data when using SNMP with VRFs configured and polling for the IP-FORWARD-MIB.

  Conditions: The symptom is observed on a Cisco Catalyst 6000 series switch that is running Cisco IOS Release 12.2(33)SXH.

  Workaround: There is no workaround.

- CSCsx83443

  Symptoms: ISKMP debug messages from all peers are shown in the terminal monitor enable tty/vtys even though **debug crypto condition peer ipv4 x.x.x.x** is set.

  Conditions: Use peer IP-based debug condition.

  Workaround: There is no workaround.

- CSCsx93245

  Symptoms: A Cisco router may reload after issuing the **show gatekeeper zone prefix all** command.

  Conditions: This symptom is observed on a Cisco 3825 router running Cisco IOS Release 12.4(8a).

  Workaround: There is no workaround.

- CSCsy20998

  Symptoms: A memory leak is observed.

  Conditions: This symptom occurs when codenomicon test is run.

  Workaround: There is no workaround.

- CSCsy32754

  Symptoms: A router acting as LNS crashes while sending packet to flapping client connected to LAC.

  Conditions: This symptom is seen with a timing issue.

Workaround: There is no workaround.

- CSCsy86078

  Symptoms: Router crashes with memory corruption.

  Conditions: This symptom is observed when BFD is configured

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm

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

- CSCsz70049

  Symptoms: A VIC2-2BRI port may go down suddenly by not detecting the RR command/response from the TELCO side, and it stays in a down state. As a result, this BRI port does not send/receive a voice call.

  Conditions: The symptom is observed on a Cisco 3825 router with VIC2-2BRI.

  Workaround: Issue the **clear interface bri** command to restore this state.

- CSCsz71787

  Symptoms: A router crashes when it is configured with DLSw.

  Conditions: A vulnerability exists in Cisco IOS software when processing UDP and IP protocol 91 packets. This vulnerability does not affect TCP packet processing. A successful exploitation may result in a reload of the system, leading to a denial of service (DoS) condition.

  Cisco IOS devices that are configured for DLSw with the **dlsw local- peer** command automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the **dlsw local-peer peer-id** *IP- address* command listens for IP protocol 91 packets and UDP port 2067.

Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
dlsw remote-peer 0 fst <ip-address>
```

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the device from receiving and processing incoming UDP packets.

Workaround: The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067, or filters can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is used only if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
dlsw remote-peer 0 fst <ip-address>
```

If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

1. Disable UDP outgoing packets with the **dlsw udp-disable** command
2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

* Using Control Plane Policing on Affected Devices

Control Plane Policing (CoPP) can be used to block untrusted DLSw traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Deny DLSw traffic from trusted hosts to all IP addresses
!--- configured on all interfaces of the affected device so that
!--- it will be allowed by the CoPP feature.

access-list 111 deny udp host 192.168.100.1 any eq 2067 access-list 111 deny 91 host
192.168.100.1 any

!--- Permit all other DLSw traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature.

access-list 111 permit udp any any eq 2067 access-list 111 permit 91 any any

!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
!--- traffic in accordance with existing security policies and
!--- configurations for traffic that is authorized to be sent
!--- to infrastructure devices.
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature.

class-map match-all drop-DLSw-class match access-group 111
```

```
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
```

```
policy-map drop-DLSw-traffic class drop-DLSw-class drop
```

```
!--- Apply the Policy-Map to the Control-Plane of the
!--- device.
```

```
control-plane service-policy input drop-DLSw-traffic
```

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function. Please note that in the Cisco IOS 12.2S and 12.0S trains, the policy-map syntax is different:

```
policy-map drop-DLSw-traffic class drop-DLSw-class police 32000 1500 1500
conform-action drop exceed-action drop
```

Additional information on the configuration and use of the CoPP feature is available at:

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

* Using Infrastructure ACLs at Network Boundary

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. iACLs are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example shown below should be included as part of the deployed infrastructure access-list that will protect all devices with IP addresses in the infrastructure IP address range. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Permit DLSw (UDP port 2067 and IP protocol 91) packets
!--- from trusted hosts destined to infrastructure addresses.
```

```
access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK eq 2067
access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
```

```
!--- Deny DLSw (UDP port 2067 and IP protocol 91) packets from
!--- all other sources destined to infrastructure addresses.
```

```
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067 access-list 150
deny 91 any INFRASTRUCTURE_ADDRESSES MASK
```

```
!--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
!--- with existing security policies and configurations.
!--- Permit all other traffic to transit the device.
```

```
access-list 150 permit ip any any
```

```
interface serial 2/0 ip access-group 150 in
```

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

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

Further Problem Description: This vulnerability occurs on multiple events to be exploited. It is medium complexity in order to exploit and has never been seen in a customer environment.

- CSCsz83570

  Symptoms: SSH sessions disconnect during large data exchanges, such as large logs with pagers.

Conditions: The symptom is observed when large amounts of data are exchanged between both ends: client and server (i.e.: the client provides a large input to the server and the server has a large output to send to the client). The session gets hung momentarily and disconnects after the timeout period of 120 seconds.

Workaround: Use 3DES for encryption.

- CSCta22767

  Symptoms: A Cisco router may crash when unconfiguring class-map.

  Condition: This symptom is observed in a Cisco router using Cisco IOS Release 15.0M.

  Workaround: There is no workaround.

- CSCta36701

  Symptoms: A group member with VSA runs out of memory and starts dropping traffic after 12 hours.

  Conditions: This symptom is observed when the packet size of the traffic sent is near mtu so that the packets get fragmented before encryption. Crypto map on a multilink interface with VSA as the crypto engine will cause memory leak for every packet decrypted.

  Workaround: Disable VSA.

  Further Problem Description: This is specific to Crypto map on a multilink interface with VSA as the crypto engine. This is not specific to a GETVPN config.

- CSCta37063

  Symptoms: NAT fails to translate H323 payload information.

  Conditions: This symptom occurs when NetMeeting is dialing from outside NAT to inside NAT.

  Workaround: Initiate NetMeeting again. Note that once this NAT entry is cleared or has timed-out, the issue will reappear.

- 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.

- 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.

- CSCtb38432

  Symptoms: EZVPN gets hung on a Cisco 871 router that is running Cisco IOS Release 12.4(24)T.

  Conditions: The symptom is observed when PPPoE renews the IP address and hangs at the "More" prompt.

  Workaround: Reconfigure the EZVPN command.

- 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.

- CSCtc46304

  Symptoms: Ping sweep and application-level traffic fail to go through, and connectivity is subsequently lost.

  Conditions: This symptom is observed when BFD and shaping are configured on the SHDSL interface.

  Workaround: After connectivity has been lost, flap the link to restore connectivity.

- CSCtc59535

  Symptoms: The DSL link stops passing traffic. The issue does not get resolved by shut and no shut of ATM interface or reloading the router.

  Conditions: The symptom is observed when the CU has a Cisco 2821 router that is running Cisco IOS Release 12.4(15)T8 with HWIC-2SHDSL.

  Workaround: Unplug and plug back the cable.

- CSCtd31084

  Symptoms: GSM-AMR CODEC cannot be disabled on a Cisco MGCP gateway when using iLBC. The CODEC will be selected regardless and then rejected due to lack of license.

  Conditions: This symptom is observed under the following conditions:

  - iLBC is in use
  - GSM-AMR is not licensed for use
  - GSM-AMR is in SDP

  Workaround: Disable CODEC on the gateway CODEC choice list. Note that this option is not always possible.

- CSCtd31465

  Symptoms: An H323 to SIP CUBE may get stuck in a race condition if a reINVITE with delayed media is quickly followed by a reINVITE with early media while still renegotiating the H323 side of the call for the delayed media INVITE. This may lead to one-way or no-way audio.

  Conditions: This symptom was observed with the following topology:

  ```
  IP phone---CUCM---H.323 Fast Start---CUBE---SIP---3rd-party SIP server--- CallCenter
  ```

  Calls flow from the IP phone to the CallCenter hanging off a 3rd-party device. The 3rd-party device re-INVITEs, rapidly, as calls traverse through its menu/IVR system.

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtd43168

  Symptoms: A breakpoint exception crash occurs while configuring SNMP traps via Cisco Works after the following errors are displayed:

  ```
  %SNMP-5-WARMSTART: SNMP agent on host <host name> is undergoing a warm start
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk ########, data ########.
  -Process= "NAT MIB Helper", ipl= 0, pid= 277
  -Traceback=
  ```

  Conditions: This symptom is observed after unconfiguring snmp-server, then configuring it again. Commands used for this configuration could include **snmp-server enable traps** or **snmp-server community**.

  Workaround: There is no workaround.

- CSCtd47338

  Symptoms: The following error message is constantly displayed:

  ```
  crypto_engine_ps_vec(): no subblock attached
  ```

  Conditions: This issue is observed on a Cisco 7200 series router with VSA cards, that is running Cisco IOS Release 12.4(15)T (other releases may be affected as well) and with DLSw configuration.

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

- CSCtd59027

  Symptoms: The device crashes due to a bus error.

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

  Workaround: There is no workaround.

- 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.

- CSCtd67940

  Symptoms: A Cisco router may crash while traffic is flowing through the ATM AIM interface.

Conditions: This symptom is observed when a QoS configuration is copied/modified which affects the ATM AIM interface while (even minimal) traffic is flowing through the ATM AIM interface.

Workaround: Stop the traffic (use the **show** command during a maintenance window, for example), copy the configuration, make sure the interface comes up with the new configuration, then restart traffic.

- CSCtd78209

  Symptoms: A Cisco router crashes when crypto is configured with ip-multicast fast switching.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(15)T12.

  Workaround: There is no workaround.

- CSCtd86472

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-nat.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCte03209

  Symptoms: On a Cisco 7206/NPE-G2 configured for IRB and L2TP, ingress ARP requests and replies may fail with this message according to “debug arp”:

  ```
  IP ARP: sent req src 10.10.10.2 0000.0c4d.4a20,dst 10.10.10.1 0000.0000.0000 BVI1
  IP ARP rep filtered src 10.10.10.1 000c.85ae.2e00, dst 10.10.10.2 0000.0c4d.4a20 wrong
  cable, interface Virtual-Access5.
  ```

  Conditions:

  ```
  bridge irb
  bridge 1 protocol ieee
  bridge 1 route ip
  interface BVI1 ip address 10.10.10.2 255.255.255.0 ip directed-broadcast
  interface Virtual-Template1 no ip address no peer default ip address ppp
  authentication pap chap bridge-group 1 bridge-group 1 spanning-disabled end
  interface Virtual-Access5 no ip address no peer default ip address ppp authentication
  pap chap bridge-group 1 bridge-group 1 spanning-disabled
  ```

  This symptom is observed on Cisco IOS Release 12.4(15)T7, Release 12.4(15) T9, and Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCte07666

  Symptoms: A Cisco router may crash when the TCL script without_completion.tcl is run.

  Conditions: This symptom is observed when running the TCL script without_completion.tcl as the script tries to fill in the _cerr_name field with an array that is not sufficiently populated.

  Workaround: There is no workaround.

- CSCte08720

  Symptoms: %SERVICE_MODULE-4-WICNOTREADY: Unit Serial0/0/0 is not ready for next command, “show service-module” counters are not accessible. In some cases the interface will remain down/down.

  Conditions: This symptom occurs when HWIC-1DSU-T1 or WIC-1DSU-T1-V2 is installed on a system that is running one of the following Cisco IOS Releases: 12.4(20)T4, 12.4(22)T3, 12.4(24)T2, 15.0(1)M2.

  Workaround: There is no workaround.

- CSCte17284

  Symptoms: A router may unexpectedly reload due to software forced crash because of chunk memory corruption.

  Conditions: The crash appears to happen when using the clientless web proxy method. The crash is triggered by accessing a webpage through the SSL VPN with a URL longer than 1009 characters long.

  Workaround: If possible, redesign the website to use URLs of 1009 characters or shorter.

- CSCte18124

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

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

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

- CSCte49283

  Symptoms: Sometimes the LNS router sends an incorrect NAS-Port value.

  Conditions: The symptom is observed when the LNS router sends a stop accounting-request to the RADIUS server.

  Workaround: There is no workaround.

- 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.

- CSCte83779

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router may crash.

  Conditions: The symptom is observed when DMVPN is configured with GETVPN. It is only seen when running a specific script for ASRs.

Workaround: There is no workaround.

- CSCtf04954

  Symptoms: When the **cns config notify** command exists, some CLIs might misbehave or cause unexpected crashes during the configuration change.

  Conditions: The symptom is observed with the **cns config notify** command.

  Workaround: Remove all **cns config notify** CLIs from the configuration.

- CSCtf13014

  Symptoms: A DNS server on a router does not immediately serve its own primary zone, if next-layer DNS servers are configured (every query is forwarded to these servers first).

  Conditions: The symptom is observed when next-level (parent) DNS servers are configured on the router.

  Workaround: There is no workaround.

- 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.

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-nat.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtf18077

  Symptoms: A CME router may unexpectedly reload due to a bus error when a Cisco Unified Contact Center Express (UCCX) unregisters from the CME.

  Conditions: The symptom is observed when the Cisco UCCX unregisters from the CME.

  Workaround: There is no workaround.

- CSCtf19461

  Symptoms: IP address is not leased out to the client from server.

  Conditions: The symptom is observed when configuring the VPN sub-option at the interface level on the relay.

  Workaround: There is no workaround.

- CSCtf25508

  Symptoms: ISAKMP profiles cannot be removed. The following error message is shown:

  ```
  %Profile is applied to Virtual-Access2-head-0/65536 and possibly other crypto maps
  ```

Note: The “2” in the error message will differ based on your configuration. In the above message, “Virtual-Access2” is referenced because the VTI number, in this case, is 2.

This keeps many stale dynamic crypto map entries without any valid IPSec SA or virtual access interfaces.

Conditions: The symptom is observed under the following conditions:

- Using VTI with EzVPN.
- Only seen with Cisco IOS Release 12.4(24)T.

Workaround: Reload the router to release the hung virtual-access sessions.

- CSCtf27324

  Symptoms: A ping from a CPE (which is doing PPP to the IP address of the LNS router that terminates that PPP call) fails. PPP has been opened and IPCP has negotiated an IP address. Ping from the LNS back to the CPE works fine. Between the LAC and the LNS there is a PPP multilink bundle.

  Conditions: The symptom is observed only when there is a plain PPP call from a client (ISDN modem or dial up modem which is doing PPP). In addition, the physical connectivity between the LAC and the LNS is PPP multilink.

  Workaround: Disable CEF on the physical interface between the LAC and the LNS. If the CPE is doing PPP multilink, the ping works fine.

  Further Problem Description: The issue seems to be specific with the forwarding of the packets through the PPP multilink bundle that exists between the LAC and the LNS.

- CSCtf31067

  Symptoms: There is no implementation for retransmitting MS-CHAP v2 challenge for PPP negotiation.

  Conditions: The symptom is observed with a MS-CHAP v2 challenge.

  Workaround: There is no workaround.

- CSCtf36117

  Symptoms: Crash occurs when executing the **show crypto session brief** command with multiple IKEv2 tunnel connections.

  Conditions: The symptom is observed when setting up as many as 500 IKEv2 tunnels employing symmetric RSA-Sig based authentication with CRL check enabled. This crash occurs when there are about 450 tunnels established and the command is trying to list down the sessions.

  Workaround: There is no workaround.

- CSCtf39455

  Symptoms: Router can hang when xconnect configuration is modified on a VLAN subinterface while data packets are being switched. The following error traceback is printed:

  ```
  %SYS-2-NOTQ: unqueue didn't find 0 in queue
  ```

  Conditions: The symptom is observed when the VLAN subinterface is still seeing data traffic and the main interface is not shut down, and when the xconnect configuration on the VLAN subinterface is being modified.

  Workaround: Shut down the main ethernet interface when doing xconnect configuration changes on the subinterface.

- CSCtf40731

  Symptoms: A routing loop is unexpectedly formed when PIRO and an OER-generated static route works together.

  Conditions: The symptom is observed under the following conditions:

  1. PIRO generates a more specific prefix for the static route it has created.
  2. OER-generated static route is redistributed into other IGP protocol in order to get traffic.

  Workaround: There is no workaround.

- CSCtf47929

  Symptoms: Tracebacks are seen on a Cisco router when creating a udp-jitter operation with request-data size of more than 17000 bytes (super jumbo packet).

  Conditions: This symptom is observed with a large request-data size.

  Workaround: Use a request-data size value less than 17000.

- CSCtf52106

  Symptoms: There is a failure of EEM TCL scripts when using the "exit_comb" keyword for the Interface Event Detector.

  Conditions: The symptom is observed when using the "exit_comb" keyword in an EEM TCL script.

  Workaround: There is no workaround.

- CSCtf62621

  Symptoms: Unable to push the firewall down to the VDSL chipset on a Cisco 887V modem.

  Conditions: The symptom is observed on a Cisco 887V router with no startup configuration in NVRAM.

  Workaround: Perform a **write memory** and reload the router.

- CSCtf67170

  Symptoms: There is a crash due to the following error:

  ```
  %ALIGN-1-FATAL: Illegal access
  ```

  Conditions: The symptom is observed when "call monitor" is configured.

  Workaround: Remove call monitor, if interfacing with UCCX is not needed.

- CSCtf70959

  Symptoms: EzVPN client is trying to negotiate the connection with a NULL address when the outside interface is a profile-based dialer interface.

  Conditions: This situation is a corner condition. The IP address on the dialer interface will be installed as soon as the dialer negotiation completes and the dialer interface comes up. But in this case, even though the IP address is not installed the dialer interface, the API is returning TRUE and proceeds further with the EzVPN connection.

  Workaround: Use a non profile-based dialer interface.

- CSCtf71010

  Symptoms: Traffic does not flow through the hub.

  Conditions: The symptom is observed when a Cisco 3900 series router is configured for VRF-aware tunnel protection for IKEv2 sessions.

  Workaround: There is no workaround.

- CSCtf71990

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

  ```
  %CALL_HOME-3-SMTP_SEND_FAILED: Unable to send notification using all SMTP servers (ERR
  7, error in connecting to SMTP server)
  ```

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

  Workaround: Remove “source-ip-address”.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm

  http://www.cisco.com/en/US/products/csa/cisco-sa-20100922-cucmsip.html

- CSCtf75053

  Symptoms: DHCP Relay will send a malformed DHCP-NAK packet. The malformed packet will be missing the END option (255) and the packet’s length will be truncated to 300. In effect, all the options after 300 bytes, if any, will be missing.

  Conditions: When a Cisco 10000 series router is configured as a relay and a DHCP request is sent from the CPE, the router will send a DHCP-NAK when client moves into a new subnet.

  Workaround: There is no workaround.

- CSCtf81271

  Symptoms: When “station-id name” or “station-id number” is configured on a voice port, “caller-id enable” will also be configured on that voice port.

  Conditions: The symptom is observed after upgrade to Cisco IOS Release 12.4(22)T or Release 12.4(24)T where the **caller-id enable** command gets auto-configured on the voice-port.

  Workaround: Manually remove the **caller-id enable** command after a router reboot.

- CSCtf82883

  Symptoms: When clearing a VRF route, there is a traffic drop on other VRF routes.

  Conditions: The symptom is observed with an L3 VPN configuration.

  Workaround: There is no workaround.

  Further Problem Description: Some LTE broker distribution is leaked to other VRFs.

- CSCtf83101

  Symptoms: Packets are not correctly classified by QoS class-map in CEF switching. Priority packets are dropped even if they are classified into LLQ. This is shown by the **show policy-map interface** command.

  Conditions: The symptom is observed under the following conditions:

  - A BRI interface.
  - LLQ is configured on egress port by policy-map.
  - The following devices/platforms are used: HWIC-4B-S/T or HWIC-1B-U, Cisco 181x, Cisco 180x, Cisco 800.

  Workaround: Disable CEF.

  Alternate Workaround: Use the other HWIC or WIC.

- CSCtf84237

  Symptoms: A router may reload with the following crash decode (traceback summary):

  ```
  0x123d7e24 is in vpdn_apply_vpdn_template_pptp
  0x1239c100 is in l2x_vpdn_template_find
  0x123d81dc is in vpdn_apply_l2x_group_config
  0x123cfedc is in vpdn_mgr_call_initiate_connection
  0x123cce68 is in vpdn_mgr_event
  0x123ce974 is in vpdn_mgr_process_client_connect
  0x123cf248 is in vpdn_mgr_process_message
  0x123cf368 is in vpdn_call_manager
  ```

  Conditions: The symptom is observed when an invalid tunnel-type VSA is configured, for example:

  vsa cisco generic 1 string "vpdn:tunnel-type=l2tp_bad"

  Workaround: Configure a correct tunnel-type VSA in Radius.

- CSCtf85219

  Symptoms: The following symptoms are seen:

  - No dial tone when going off hook, so other phone numbers cannot be dialed.
  - The hung port can receive incoming calls, however the originating phone hears ring back. The terminating phones rings but when the call connects there is one-way audio.

  Conditions: The symptom is observed with STCAPP-controlled FXS ports.

  Workaround: Perform a shut/no shut on the voice port. If this does not work, perform a reload.

- CSCtf87039

  Symptoms: Device crashes at crypto_ikmp_process_xauth_reply.

  Conditions: The symptom could occur while processing the xauth response received from the client. The PPC platform crashes (the MIPS64 platform does not crash).

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-nat.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtg08496

  Symptoms: After merge, keyserver deletes all GMs so the rekey fails to be sent (DB is empty) and all the GMs need to re-register.

  Conditions: The symptom is observed when running Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sslvpn.

Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtg23115

  Symptoms: A memory leak occurs in the Pool Manager process.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(24)T. It is not yet known what other IOS releases may be affected. This symptom is seen with multicast enabled.

  Workaround: There is no workaround to prevent the leak. Once the memory has leaked, reloading the router will temporarily free the memory.

- CSCtg23251

  Symptoms: Analog phones lock up and there is no dial tone.

  Conditions: The symptom is observed when the CME is in fallback as SRST and a directed call park is attempted on analog phones. The user cannot pick up a call from a park slot by direct dialing the slot. In the event that the user is able to retrieve the call, when the call is hung up the channel is not released. No dial tone is heard when the handset is picked up again.

  Workaround: Reset the ports.

- CSCtg40901

  Symptoms: Crash seen while authenticating with TACACS.

  Conditions: The symptom is observed if the TACACS server does not respond.

  Workaround: Use multiple connections.

  Alternate Workaround: Configure a dummy TACACS server.

- CSCtg41206

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

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

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

- 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.

- CSCtg42179

  Symptoms: High CPU utilization occurs under interrupt. CPU profiling indicates that this is due to QoS.

  Conditions: This symptom is observed on Cisco ISR 3800 routers with Cisco IOS Release 12.4(15)T10. It is not yet known what other platforms and/or versions are affected.

  Workaround: There is no workaround. A lower traffic rate may lower the CPU utilization.

- CSCtg50024

  Symptoms: A router experiences crashes due to TLB (load or instruction fetch) exception.

  Conditions: This problem is observed on a Cisco 7206VXR router with Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtg55447

  Symptoms: GETVPN keyserver TEK sequence number goes out of sync during network split/KS failure. This causes the GM to reject the older key and reregister.

  Conditions: This symptom is seen during primary keyserver failure or network failure between primary keyserver and secondary keyserver.

  Workaround: There is no workaround.

- CSCtg57623

  Symptoms: Music on hold does not work with iLBC codec when an IOS transcoder is used.

  Conditions: The symptom is observed when the phone is configured to use iLBC codec and a transcoder is invoked to transcode MOH G.711 audio stream to iLBC codec. The phone rejects the RTP stream due to incorrect payload-type (it sends payload type 118 instead of the correct 116 for iLBC).

  Workaround: There is no workaround if iLBC codec is needed, but using a different codec at the remote phone should work.

- CSCtg57657

  Symptoms: A router is crashing at DHCP function.

  Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.

  Workaround: There is no workaround.

- 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.

- CSCtg68208

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

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

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

- CSCtg69202

  Symptoms: CUBE modifies the RTP port number before passing it to the remote end, which causes one-way audio.

  Conditions: This symptom is observed only when the RTP port number is higher than the RTCP port number in the incoming request from the endpoint. Instead of sending the same RTP port number, CUBE decrements the RTP port number by one less than the RTCP port number when it forwards the OLC Ack to the destination side. This causes the destination to send the audio packets to the wrong port on the originating side, causing one-way audio.

  Workaround: There is no workaround.

  Further Problem Description: Under some specific conditions, when CUBE receives the OLC acknowledgement with the media control information from an H323 client, instead of passing the same RTP port number to the remote end, it modifies the RTP port number, causing the one-way audio.

- CSCtg71332

  Symptoms: On a Cisco 3800 ISR that is using NM-1T3/E3 module, the controller will be down/down should following condition be true.

  Conditions: This symptom has been noticed on the router that is running Cisco IOS Release 12.4(15)T8 with advanced IP services or IP services feature set.

  Workaround:

  1. Use SP services feature set.
  2. Upgrade router to Cisco IOS Release 12.4(24)T.
  3. Install one or more PVDM sLOTS.

- CSCtg88766

  Symptoms: HWIC-SHDSL does not train up in 4-wire standard mode.

  Conditions: The symptom is observed when CPE is in 4-wire standard mode and the DSLAM line card is GSPN-based and configured in 4-wire standard mode.

  Workaround: There is no workaround.

- CSCtg92783

  Symptoms: Uplink performance degrades by about 70% with HWIC-3G-CDMA when bound to external dialer interface when compared to using cellular interface legacy DDR.

  Conditions: This symptom is seen on live network when performance is measured using latency sensitive Internet speed test application.

  Workaround: Use cellular interface without binding to external dialer.

- CSCtg93243

  Symptoms: QoS + tunnel protection does not work if UUT2 is running VSA. Packets get dropped at UUT2 after being decrypted by VSA.

Conditions: The symptom is observed with crypto, tunnel protection, and VSA only. (If static crypto + VSA, or tunnel protection + SW crypto is used packets get forwarded after decryption as expected.)

Workaround: There is no workaround.

- CSCth01939

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

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

  Workaround: There is no workaround.

- CSCth33457

  Symptoms: A Cisco IOS router configured with IPSec (IP Security) may reload when receiving encrypted packets.

  Conditions: This symptom is observed when one or more of the following is configured on an interface configured with IPSec:

  - ip accounting precedence input
  - ip accounting mac-address input
  - WCCP -Flexible NetFlow
  - BGP accounting
  - uRPF
  - mpls accounting experimental input

  Workaround: Avoid using IPSec or avoid using all of the above features on the interface.

- CSCth33500

  Symptoms: NAS port is reported as zero on LNS.

  Conditions: This symptom occurs when “vpdn aaa attribute nas-port vpdn-nas” is configured.

  Workaround: There is no workaround.

- CSCth36261

  Symptoms: A router crashes.

  Conditions: This symptom occurs when the router is configured for fax calls (specific to T.37 only).

  Workaround: There is no workaround.

- CSCth63379

  Symptoms: With two T1 links running ATM with IMA bundling, the proper CEF- attached adjacency for the opposite end of the link does not appear.

  Conditions: This symptom is observed on a Cisco 3800 series device with VWIC- 2MFT-T1.

  Workaround: There is no workaround.

- 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 a Cisco IAD243x using a HWIC-CABLE-D-2.

  Workaround: Manually change the MAC address problem card.

Further Problem Description: The same card works correctly on a Cisco 1841 router with the default MAC address from the Cisco 1841.

- 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.

- CSCti15990

  Symptoms: EzVPN will not come up if the dialer interface flaps.

  Conditions: This symptom is observed when the dialer interface is profile-based.

  Workaround: Change the dialer interface to non-profile-based.

Resolved Caveats—Cisco IOS Release 12.4(24)T3

Cisco IOS Release 12.4(24)T3 is a rebuild release for Cisco IOS Release 12.4(24)T. The caveats in this section are resolved in Cisco IOS Release 12.4(24)T3 but may be open in previous Cisco IOS releases.

- 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 best-path calculations.

- 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.

- CSCsu50869

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

  Conditions: This symptom 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.

- CSCsw39413

  Symptoms: The following sequence of steps used to reset all the C5510 DSPs on a Cisco 1861 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 1861 voice gateways that are 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 that is running Cisco IOS software is interoperating with a router that is 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, this problem is seen.

  Workaround: There is no workaround.

- CSCsw79891

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

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

  Workaround: There is no workaround.

- 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.

- CSCsy30256

  Symptoms: A Cisco 2811 router crashes due to a bus error after an ISDN call terminates. The following is seen before the crash:

```
%ALIGN-1-FATAL: Corrupted program counter pc=0x0 , ra=0x400ABA78 , sp=0x44647440
TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x0
```

  Conditions: The symptom is observed when "dialer rotary-group <number>" is configured on the interface.

  Workaround: Use "dialer pool" instead of "dialer rotary".

- CSCsy41063

  Symptoms: A Cisco router may display the following error message:

```
%SYS-2-BADBUFFER: Attempt to use Mismatch sized buffer as scattered src, ptr=
83BB71E0, pool= 83A4F670 -Process= "<interrupt level>", ipl= 2, -Traceback= 0x808DA290
0x80087808 0x801BAF9C 0x800E5954 0x800E73F0 0x80369148 0x8008590C 0x8008590C
0x80369208 0x8036D334 0x81957024 0x8036B57C 0x80375294
```

  Conditions: This symptom is observed with a Q-in-Q configuration on the device.

  Workaround: There is no workaround.

- CSCsy61321

  Symptoms: Accounting requests sent to the TAC server do not fail over to the second server.

  Conditions: This symptom is observed when two TACACS servers are configured, the first without TACACS, the second with TACACS, and authentication is configured as "none".

  Workaround: Use a single working server, or ensure that the first group uses a valid server.

- CSCsy74023

  Symptoms: A slow memory leak occurs, mainly in the 72 bytes, 80 bytes, and possibly 192 bytes memory regions blocks.

  Conditions: This symptom is observed with a large number of IPSec peers (more than 100) and several thousand tunnels when Phase I is authenticated by RSA-SIG.

  Workaround: There is no workaround.

- 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/en/US/products/csa/cisco-sa-20100324-cucme.html.

- CSCsz62974

  Symptoms: A router crashes while querying for cvpdnTemplateActiveSessions.

  Conditions: This symptom occurs if the vpdn-template name is long.

  Workaround: There is no workaround.

- 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 a service policy also.

  Workaround:

  1. Do a **shut/no shut** on the affected interface.

  2. Do a soft OIR on 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.

- CSCsz97833

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

  Conditions: This symptom occurs due to an extra character appended to the URL.

  Workaround: Disable CRL checking.

- 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.

- CSCta09049

  Symptoms: A memory leak chunk in alloc-proc "encrypt proc" with the name "Packet Header" is observed.

  Conditions: This symptom is observed with software crypto enabled. The same configuration and traffic running with onboard-VPN does not have the leak.

  Workaround: Configure the "no ip cef optimize neighbor resolution" command.

- 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.

- CSCta18454

  Symptoms: CN is unable to ping MN due to a tunnel failure on the HA.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.4(15)T10.

  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/en/US/products/csa/cisco-sa-20100324-h323.html.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-sip.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090826-cucm

http://www.cisco.com/en/US/products/csa/cisco-sa-20100922-cucmsip.html

- CSCta20590

  Symptoms: A group member (GM) pseudotime may desynchronize after re-registering or at initial registration.

  Conditions: This symptom is observed when GETVPN with time-based anti-replay (TBAR) is enabled.

  Workaround: Disable TBAR or use a very large window (greater than 30 seconds).

  Further Problem Description: After establishing phase I, the GM is supposed to obtain the KEK and TEKs. If a packet drop occurs (usually, this message is fragmented across multiple frames), then the router is not able to reassemble the packet. IKE will later resend this message, but if the pseudotime has not been recalculated the symptom will reoccur.

- CSCta32825

  Symptoms: A Cisco router may crash with a bus error after configuring a class-map or modifying a class-map.

  Conditions: This symptom is observed when using the **class-map** command in global configuration mode and the **match** command in class-map configuration mode. For example, entering the following commands may result in a crash:

```
Router(config)# class-map match-any PRIO
Router(config-cmap)# match dscp cs4
Router(config-cmap)# match dscp cs4 af41
Router(config-cmap)# match dscp cs4 af41 af42
Router(config-cmap)# match dscp cs4 af41 af42 af43
Router(config-cmap)# match dscp cs4 af41 af42 af43 ef
Router(config-cmap)# match dscp cs4 af41 af42 af43 ef cs5 <---device crashes here
```

  Workaround: Configure QoS changes when no traffic is passing through the router. This has been seen only while traffic is trying to match against the policy while it is being updated.

- 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.

- CSCta63555

  Symptoms: A router crashes if running with Cisco IOS Release 12.4(24)T or later.

Conditions: The symptom is observed if the SNR number change menu is selected from an extension mobility phone. The router crashes after submitting the change.

Workaround: Configure an SNR under the user-profile or logout-profile with which the extension mobility phone is provisioned.

- 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.

- CSCta69213

  Symptoms: A Cisco router that is configured for NHRP may crash due to a bus error.

  Conditions: This symptom is observed on a Cisco router that is configured for NHRP and DMVPN.

  Workaround: There is no workaround.

- CSCta73534

  Symptoms: In rare cases, copying a file to Cisco IOS via the Cisco IOS SCP server fails, but the SCP server returns an OK (0) code. The file that failed to copy appears on the router as zero bytes.

  Conditions: This symptom occurs when the SCP server does not receive an EOF marker from the SCP client.

  Workaround: There is no workaround.

- 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.

- CSCta86675

  Symptom: A Cisco router may crash and report 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.

- CSCta93129

  Symptoms: An IP fragment may bypass virtual fragment reassembly (VFR) processing and create a VFR timeout, causing additional inner IP fragments to be dropped.

  Conditions: This symptom is observed when encrypted IPSEC packets are fragmented by the remote device (fragmentation after encryption) or somewhere in the network between the VPN termination routers. When the fragmented IPSEC packets are reassembled and decrypted, if the decrypted inner packet is also an IP fragment, the IP fragment bypasses VFR processing. The following conditions may cause this symptom to occur:

  1) VFR is enabled on the decryption side.

  2) Fragmentation happens after encryption on the encrypting router, or in the path.

  3) The inner IP packet is fragmented when received by the encrypting router.

Workaround: Perform fragmentation before encryption on the sending side, and ensure that the proper IP MTU is used on the tunnel so that no fragmentation occurs after encryption.

Further Problem Description: When IPSEC packets corresponding to the first inner IP fragment bypass VFP processing, the second inner IP fragment, even if too small to require IPSEC fragmentation, is decrypted and then sent for VFR processing. Due to the timeout created when the first IP fragment bypasses VFR processing, the second inner IP fragment is dropped.

- 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.

- CSCtb21428

  Symptoms: An interface does not attempt to restart after restart-delay is configured.

  Conditions: When the serial interface is down for some reason and you have configured restart-delay on the serial interface, the interface should try to restart.

  Workaround: There is no workaround.

- CSCtb22889

  Symptoms: SIP(TLS--SIP CUBE) may experience up to 2 to 3 seconds of post-dial delay due to TLS processing. Processing delays of 1000 ms, 600 ms, and 200 ms are seen between the gateway TLS responses.

  Conditions: This symptom is observed with a TLS connection to another gateway.

  Workaround: Use the **sip-ua timers connection aging tls** *time* command to increase the time in the gateway TLS aging timer and therefore lower the frequency of the problem with the aging TLS timer.

- 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 instead.

- CSCtb45057

  Symptoms: A fax through a Cisco IOS gateway configured for Fax Relay to a Cisco fax server fails.

  Conditions: When there is an incoming fax call on the Cisco IOS gateway that is configured for Fax Relay, the fax call setup between the gateway and the Cisco fax server fails. This symptom occurs when the Cisco fax server is configured to receive calls on an H.323 call control module.

  Workaround: There is no workaround. Configure SIP between the Cisco IOS gateway and the Cisco fax server if that is an acceptable workaround.

- CSCtb45718

  Symptoms: A Cisco router may crash with traceback leading to checkheap.

  Conditions: This symptom is observed when endpoint agnostic port allocation has been enabled using the **ip nat service enable-sym-port** command.

  Workaround: Disable the endpoint agnostic port allocation using the **no ip nat service enable-sym-port** command.

Further Problem Description: Under certain conditions, the symmetric port database is not in sync with the port list, resulting in the reuse of port ranges that had been free.

- CSCtb48397

  Symptoms: A Cisco ISR router may experience performance degradation due to corrupted TCP headers.

  Conditions: This symptom is observed on a Cisco ISR router with Cisco IOS Release 12.4 or Release 12.4T running interface-based TCP header compression on any data link. Corrupted TCP headers may occur when all of the following are true:

  1. Frame-Relay, PPP, or HDLC is configured with “ip tcp header-compression”.

  2. The queueing mechanism is fair-queue (either interface-based or in map-class frame-relay).

  3. More than 1 TCP sessions are traversing the compressing mechanism.

  4. The packets are in the hardware (CEF) switching path.

  Workarounds:

  1. Do not configure an interface to carry compressed TCP/IP headers using the **frame-relay ip tcp header-compression** command.

  2. Disable hardware switching for all interfaces on the Cisco ISR using the **no ip route-cache** command.

  3. Do not use any form of fair-queue on interfaces configured with the **frame-relay ip tcp header-compression** command. To remove fair-queue, use the **no fair-queue** command in policy-map class configuration mode.

  Further Problem Description: With exactly two MS Remote Desktop Protocol TCP sessions, when the UUT’s serial transmit-ring (or frame-relay shaper Bc) congests and the fair-queue invokes, the compressed header from the second- established TCP flow is erroneously written into headers of some packets from the first-established TCP flow, resulting in post-decompression frames erroneously added to the first-established TCP flow and erroneously removed from the second-established TCP flow, thereby causing a performance degradation.

- 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.

- CSCtb60603

  Symptoms: The router crashes and resets when you try to execute the following command:

  show run | format *x* (where x = any keyword)

  Conditions: The symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(24)T. The router needs to have a general route map configured.

  Workaround: Do not execute **show run | format** *x* if there is a general route map configured in the router.

- CSCtb66963

  Symptom: A SIP call from a call-forwarded phone to a Cisco IOS VoIP gateway is rejected when the INVITE contains a comma in the Diversion Header.

  Conditions: The following is an example of an inbound SIP invite that contains a Diversion field such as this:

  ```
  ---- Received: INVITE sip:15551111111@10.1.134.116:5070 SIP/2.0 Via: SIP/2.0/UDP
  172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 Remote-Party-ID:
  <sip:5555555555@172.27.128.130>;party=calling;screen=yes;privacy=off From:
  <sip:5555555555@172.27.128.130>;tag=c565ee9d-7f0b-49dd-a1d9- 3843c1b221cc-53184879?
  To: <sip:15551111111@10.1.134.116> Date: Sat, 29 Aug 2009 08:06:56 GMT Call-ID:
  e9edd580-a981e1a0-109-82801bac@172.27.128.130 Supported: timer,replaces Min-SE: 1800
  User-Agent: Cisco-CCM5.1 Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK,
  UPDATE, REFER, SUBSCRIBE, NOTIFY CSeq: 101 INVITE Contact:
  <sip:5555555555@172.27.128.130:5070> Expires: 180 Allow-Events: presence
  Session-Expires: 1800 Diversion: "Smith, John"
  <sip:87007@172.27.128.130>;reason=unconditional;privacy=off;screen=no Max-Forwards: 7
  Content-Type: application/sdp Content-Length: 214 ----
  ```

  The Cisco IOS gateway will respond with the following:

  ```
  ---- Sent: SIP/2.0 400 Bad Request - ’Malformed CC-Diversion/Diversion/CC-Redirect
  Header’ Reason: Q.850;cause=100 From:
  <sip:5555555555@172.27.128.130>;tag=c565ee9d-7f0b-49dd-a1d9- 3843c1b221cc-53184879
  Content-Length: 0 To: <sip:15551111111@10.1.134.116>;tag=B8C0430-6C Call-ID:
  e9edd580-a981e1a0-109-82801bac@172.27.128.130 Via: SIP/2.0/UDP
  172.27.128.130:5070;branch=z9hG4bK1432a4c26c3 CSeq: 101 INVITE ----
  ```

Workaround: Modify the diverting name associated with the redirecting device so that it does not contain a comma.

- 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 flash instead of to an FTP URL.

- CSCtb82256

  Symptoms: A Cisco router may crash.

  Conditions: This symptom is observed when *all* of the following occur:

  - Cisco Unified CallManager XML configuration files are downloaded to the router while the router is processing the pri-group configurations.
  - The **shutdown** and **no shutdown** commands are entered on the voice port.
  - The **no ccm-manager** command is entered.

  Workaround: Do not shut down the voice port at the time of configuration download.

- CSCtb89424

  Symptoms: In rare instances, a Cisco router may crash while using IP SLA UDP probes that are configured using SNMP and may 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.

- CSCtc04016

  Symptoms: A Cisco IOS VoIP gateway configured for IPIPGW/CUBE may experience high CPU utilization, which causes additional calls through the router to fail.

  Conditions: This symptom is observed under rare conditions when SIP-associated processes on the Cisco IOS gateway (as seen when the **show process cpu** command is entered) cause extremely high CPU utilization, which causes further calls through the router to fail.

  Workaround: There is no workaround.

  Further Problem Description: This symptom occurs due to a SIP “491 Request Pending” and ACK loop between the gateway and a third-party device. This loop most often occurs in environments with a large number of SIP REFER transfers. To determine whether the loop is occurring, enter the **show sip statistics** command and look for the RequestPending value; a high and increasing output count could indicate the SIP loop.

- CSCtc11521

  Symptoms: Invalid pointer value is displayed whenever NVRAM is accessed.

  ```
  "NV: Invalid Pointer value(460E460C) in private configuration structure"
  ```

  Conditions: This symptom is observed when upgrading NVRAM from an older version to a newer version.

  Workaround: Load a prior working image and backup all files in NVRAM, including the startup-config, to another device or tftp/ftp. Load the new image and enter the **erase/all nvram** command followed by the **write mem** command. NVRAM will now be restored. Copy the backup files back to NVRAM.

- CSCtc12312

  Symptoms: PKI might get stuck after 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.

- CSCtc17162

  Symptoms: A Cisco router may crash due to a SegV exception.

  Conditions: This symptom is observed on a Cisco 2650XM router that is running Cisco IOS Release 12.4(15)T10 when VTI is configured inside the EzVPN.

  Workaround: Remove the VTI inside the EzVPN.

- CSCtc18562

  Symptoms: When Network Address Translation (NAT) of the outside source address is enabled, the static route to the local IP address is installed in the global RIB instead of the VRF RIB.

  Conditions: This symptom is observed when enabling NAT of the outside source address using the **ip nat outside source static** *global-ip local-ip* **vrf** *vrf-name* **add-route extendable match-in-vrf** command.

  Workaround: Configure a static route within the VRF.

- CSCtc28059

  Symptoms: HTTP CORE process might start consuming 99 percent of a Cisco router's CPU time.

  Conditions: This symptom is observed on Cisco ISR routers that are running Cisco IOS Release 12.4(24)T1 when Cisco IOS content-filtering is active and the reputation server is unreachable (that is, timing out during a three-way handshake of the registration SSL connection).

  Workaround: Disable the URL content-filtering.

- CSCtc32374

  Symptoms: ISDN Layer 1 is deactivated after a reload, and calls fail with cause code 47 (Resource Unavailable).

  Conditions: This symptom is observed when the **busyout monitor** command is configured and the TEI controller comes up before the monitored interface.

  Workaround: Remove the busyout monitor configuration using the **no busyout monitor** command in voice-port configuration mode.

  Further Problem Description: Entering the **shutdown** command followed by the **no shutdown** command will bring PRI Layer 1 to Active and Layer 2 to a MULTIFRAME-ESTABLISHED connection status, but calls still fail with cause code 47.

- CSCtc51539

  Symptoms: A Cisco router crashes with a "Watch Dog Timeout NMI" error message.

  Conditions: This symptom is observed only on devices that are configured with Bidirectional Forwarding Detection (BFD). For further information on BFD, consult the following link:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

  Workaround: Disable BFD.

- CSCtc51573

  Symptoms: CME group pickup or pickup features do not work properly.

  Conditions: This symptom is observed in Cisco IOS Release 12.4(24)T1 when a call is placed to the voice-hunt group.

  Workaround: There is no workaround.

- CSCtc58898

  Symptoms: In an MPLS VPN scenario, if it happens that default route known via RIP in VRF is looping, route might stay in RIB.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(33)SRC4 and 12.2(33)SRC5.

  Workaround: Clear the VRF routing table using the **clear ip route vrf** *name* * command.

- 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.

- CSCtc73759

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-h323.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- 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.

- CSCtd00054

  Symptoms: Link flap/down on PA-MC-T3E3-EC interface.

  Conditions: This symptom is observed when changing encapsulation after a reload.

  Workaround: Perform an online insertion and removal (OIR) of the PA.

- 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.

- CSCtd21666

  Symptoms: Prefixes are not advertised from an MPLS VPN PE router to a group of CEs (all belonging to an update-group).

  Conditions: Found that the issue toggles between two update-groups. The only difference between the two update-groups is that one of the update-groups has the “4 octets ASN capable” set.

  Workaround: Clear the leader of the update-group that is not advertising any routes (works most of the time).

- 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 the **no supplementary-service media-renegotiate** command with no H.450 forwards.

- CSCtd23069

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

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

  Workaround: There is no workaround.

- CSCtd48005

  Symptoms: Some dialer sessions are not being freed after all calls are disconnected in an LSDO environment.

  Conditions: This symptom is observed when using SGBP (all the remaining sessions are passed to the SGBP peer).

  Workaround: Use the **clear dialer sessions** command to free the dialer sessions.

- CSCtd51715

  Symptoms: Unused links reserved for call-in are sometimes used for dial-out.

  Conditions: This symptom is observed when the **dialer reserved- links 4 0** command is configured under the dialer interface.

  Workaround: There is no workaround.

- CSCtd59174

  Symptoms: PfR MC logs an Exit Mismatch after controlling a traffic class using policy-based routing (PBR). At this point, PfR uncontrols the traffic class because it appears that traffic is not flowing over the exit interface that is expected.

  Conditions: This condition is observed under the following conditions:

  - At least one Cisco Catalyst 6000 PfR BR must by configured.
  - Monitor mode must include passive monitoring such as mode monitor both or mode monitor passive.

  Workaround: Apply mode monitor active policy to the traffic classes controlled by PBR. Note, however, that this will prevent these traffic classes from being used for load, range, or cost policies.

- CSCtd60858

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

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

  Workaround: There is no workaround.

- CSCtd63792

  Symptoms: Calls may fail to a particular B channel in a PRI with cause code 47 (resources unavailable).

  Conditions: This symptom is observed on a Cisco gateway with H.323 and PRI and Cisco IOS Release 12.4(15)T10.

  Workaround: Busy-out the affected B channel.

- CSCtd72647

  Symptoms: Severe throughput degradation out an interface occurs when a plain QoS policy map (not hierarchical, with no parent shaper) is applied.

Conditions: This symptom has been observed on Cisco integrated service routers (ISRs) with either HWIC-1FE or HWIC-2FE cards running Cisco IOS Release 12.4(20)T, Release 12.4(22)T, or Release 12.4(24)T. The symptom has not been observed in Cisco IOS Release 12.4(15)T.

Workaround: Use a hierarchical policy map with a parent shaper.

- CSCtd75189

  Symptoms: Continuous error message similar to the one below are recorded on a voice gateway:

  ```
  SYS-2-INPUTQ: INPUTQ set, but no IDB, ptr=6818DA34, -Traceback=
  ```

  Conditions: The symptom is observed on a voice gateway that is running Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtd87666

  Symptoms: The incoming MLPPP packets via the DSL interfaces are process-switched rather than CEF-switched.

  Conditions: This symptom is observed when MLPPP is configured on a Cisco 1861 integrated services router. The symptom does not occur with the same configuration on a Cisco 28xx router.

  Workaround: There is no workaround.

- CSCtd88274

  Symptoms: Secure conference resource (dspfarm) fails after a Cisco gateway is reloaded.

  Conditions: Secure conference-resources will not register after a gateway reload and shows the status unregistered in CM. The SCCP IOS configuration needs to be deleted then re-inserted to bring the resource back to a registered state. When the condition occurs, entering the **show sccp** command displays “not an active oper state” and “no active callmanager”.

  Workaround: There is no workaround.

- CSCtd94704

  Symptoms: A Cisco router may reload due to a watchdog timeout in the SCCP application.

  Conditions: This symptom is observed when the router is configured for MTP and transcoding for SCCP DSPfarms.

  Workaround: There is no workaround.

- CSCtd94789

  Symptoms: IPSEC rekey fails after failover with stateful IPSEC HA in use.

  Conditions: The symptom is observed when using PFS and after a failover of the hub devices.

  Workaround: If the security policy allows, remove the PFS to eliminate the issue.

- CSCtd94947

  Symptoms: A Cisco 2851 router that is running Cisco IOS Release 15.0(1)M and that is using the onboard HW encryption may stop processing encryption traffic after receiving a multicast packet that matches the encryption policy.

  Conditions: This symptom is observed with GETVPN encryption when the time-based anti-replay feature is turned on and when multicast traffic matches a permit statement in the encryption policy.

  Workaround: Use software-based encryption by enabling the **no crypto engine onboard 0** command in the global CLI, or disable CEF using the **no ip cef** command.

- CSCte01303

  Symptoms: New Primary KS after failover does not allow KS policy changes.

Conditions: This symptom is observed when a KS failover occurs first and then the policy change is applied on the new primary KS.

Workaround: Apply the policy change in the primary KS once it comes up, and then force a KS role re-election by entering the **clear crypto gdoi ks role** in the new primary KS. Once the previous primary KS is restored as the primary KS, apply the policy change.

- CSCte12104

  Symptoms: A crash occurs at startup with the following error message:

  ```
  %SYS-6-STACKLOW: Stack for process ATM Periodic running low, 0/9000
  ```

  Conditions: The symptom is observed when a QoS policy is applied on an ATM interface. There is no specific trigger.

  Workaround: There is no workaround.

  Further Problem Description: This issue may not be widely encountered because it is difficult to reproduce.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-igmp.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- 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 the **clear pppoe all** command is entered:

```
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 the **line-mode 4-wire enhanced** command.

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.

- CSCte19478

  Symptoms: Entering the **crypto isakmp xauth timeout** command does not seem to have any effect.

  Conditions: This symptom is observed when the command is needed for a specific scenario where user input at xauth requires more time than the default timeout value—for example, for rsa authentication (in new pin mode).

  Workaround: There is no workaround.

- CSCte21958

  Symptoms: A Cisco router may reload when an L2TP xconnect pseudowire is configured using a pseudowire class that has not yet been defined.

  Conditions: This symptom is observed when the following sequence of commands is entered:

  ```
  configure terminal
  interface Ethernet0/0.1
  encapsulation dot1Q 400
  xconnect 10.0.0.1 555 encapsulation l2tpv3 pw-class test
  pseudowire-class test *encapsulation l2tpv3
  protocol l2tpv3 test
  ip local interface Loopback0
  vpdn enable
  ```

  This symptom affects all platforms.

  Workaround: Define the pseudowire class using the **pseudowire-class** configuration command before referencing that pseudowire class in an xconnect configuration.

- CSCte23299

  Symptoms: A Cisco 877W router is not responding to IPv6 neighbor solicitation.

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCte28777

  Symptoms: A line is logged out from the hunt group if the user enables DND and then logs out with extension mobility, logs back in, and disables DND.

  Conditions: This symptom is observed when the “ephone-hunt logout DND” option is configured with EM login/logout.

  Workaround: Use the “ephone-hunt logout HLog” option instead.

- 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.

- CSCte41410

  Symptoms: TCP connections may get stuck

  Conditions: This symptom is observed when using SSLVPN with the **webvpn cef** command configured. These connections will be stuck in a TIMEWAIT state and will not time out after the usual minute or so and will stay around forever.

  Workaround: Issue the **no webvpn cef** command.

- CSCte43663

  Symptoms: RTCP packets are not forwarded across the network.

  Conditions: This symptom is observed in an IPIPGW configuration.

  Workaround: There is no workaround.

- CSCte76513

  Symptoms: If ZBF and WAAS are configured on a router, you may see drop logs similar to the following:

```
%FW-6-DROP_PKT: Dropping tcp session x.x.x.x y.y.y.y due to No zone-pair between
zones with ip ident 0
%FW-6-DROP_PKT: Dropping http session x.x.x.x y.y.y.y on zone-pair admin-to-wan
class admin due to Invalid Flags with ip ident 0
```

Conditions: The symptom is observed if ZBF and WAAS are configured on a router.

Workaround: There is no workaround.

- CSCte81855

  Symptoms: The following symptoms occur when a Cisco Voice XML (VXML) gateway reaches 2048 open sockets:

  - Dead air on call and call drops.
  - If customer has survivability TCL enabled in ingress gateway, the call will go to survivability.
  - Agents can be reserved, but voice calls do not reach the agent. Calls to the agent are placed after the original call failed, and the call is handled by survivability TCL.
  - Errors displayed in the VXML gateway are related to Network Out of Order cause code 38 and ip transfer to 0.0.0.0 ip address failed

  Conditions: This symptom is observed in any Cisco gateway, specifically Cisco 2800, Cisco 3800, and Cisco AS53. The symptom occurs in the following Cisco IOS releases:

  - 12.4 (15)T6
  - 12.4(15)T7
  - 12.4(15)T8
  - 12.4(15)T9
  - 12.4(15)T10
  - 12.4(15)T11
  - 12.4(15)T12

  Workaround:

  - Make sure that the media server and VXML server are reachable.
  - Make sure that all media files requested exist in the media server and that the path to the media file is correct.
  - Make sure that media server backup is configured in the VXML gateway (for example, ip host mediaserver-backup).
  - Check the HTTP client process using the following command:

    show proc cpu | include http client show socket *X*

    Where *X* is the ID of the HTTP client process showing with the previous command.

  If the TCP sockets are getting close to 2048, shut down the voice service voip and wait for all the IP calls to finish to reboot the gateway. If this is also an ingress gateway, you will have to re-route the calls to another ingress gateway.

- CSCtf42216

  Symptom: The **no shutdown** command will not take effect if done immediately after entering the **shutdown** command under voice-port.

  Conditions: Executing a **no shutdown** command after the **shutdown** command will not get executed immediately and will be ignored. The user has to re-enter the **no shutdown** command a few seconds later.

Workaround: Wait a few seconds to re-enter the **no shutdown** command.

Resolved Caveats—Cisco IOS Release 12.4(24)T2

Cisco IOS Release 12.4(24)T2 is a rebuild release for Cisco IOS Release 12.4(24)T. The caveats in this section are resolved in Cisco IOS Release 12.4(24)T2 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.

- 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.

- 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.

- 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.

- CSCsl52962

  Symptoms: The RP crashes due to a watchdog timeout of the uRPF stats process.

  Conditions: The symptom is observed when issuing the **interface range port-channel** <*number*> - <*number*> command.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsq42671

  Symptoms: LiveRcd softkey label is shown as "???" instead of localized string.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(15)XZ with Japanese locale.

  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.

- CSCsq83006

  Symptoms: When some port-channels go down at the same time on a router, it can cause EIGRP SIA errors.

  Conditions: The symptom occurs with full mesh four routers which are connected via port-channels. Additionally, it occurs with over five routers which are connected via a partial mesh port-channel.

  Workaround: Use the port-channel interface settings below:

  ```
  (config)# interface port-channel <port-channel interface number>
  (config-if)# bandwidth <bandwidth value>
  (config-if)# delay <delay value>
  ```

  Further Problem Description: If a test is done with a physical interface, not a port-channel, this issue is not seen.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsv30540

  Symptoms: The error message %SYS-2-CHUNKBOUNDSIB and traceback are seen.

  Conditions: The 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.

- 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.

- 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**.

- 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.

- 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.

- CSCsx05494

  Symptoms: There is a rapid memory leak.

  Conditions: The symptom is observed with a running configuration with Zone-based Firewall (ZBFW) and QOS setup.

  Workaround: There is no workaround.

- CSCsx10028

  Symptoms: A core dump may fail to write or write very slowly (less than 10KB per second).

  Conditions: The symptom is observed when the cause of the crash is processor memory corruption. When this occurs, the corrupted memory pool cannot be used to write the core dump so it will likely fail. (IO memory corruption crashes should not have this problem.)

  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.

- 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.

- 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.

- CSCsx70594

  Symptoms: A router configured for SSL-VPN and with TE tunnels may truncate packets when sending traffic from SSLVPN over the TE tunnel. This does not affect all packets, as some transmit correctly. When the issue is seen, 14 bytes are missing from the tail of the data packet.

  Conditions: The symptom is observed with SSL-VPN traffic that transmits over a TE tunnel.

  Workaround: Disable hardware encryption.

- 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.

- CSCsx80629

  Symptoms: Router with QoS configuration crashes after removing bandwidth from the policy-map.

  Conditions: The symptom is observed when the policy-map is attached to the router interface.

  Workaround: Remove the policy-map from the interface and then remove bandwidth from the policy-map.

- 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.

- 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).

- 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* command 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/en/US/products/csa/cisco-sa-20100324-sccp.html.

- 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.

- CSCsy19463

  Symptoms: A router crashes.

  Conditions: The symptom is observed with an "nhrp" configuration in an mGRE tunnel interface configuration related to NHRP/DMVPN.

Workaround: There is no workaround.

- 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.

- 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.

- CSCsy29533

  Symptoms: A T38 fax relay call may fail.

  Conditions: The symptom is observed with an MGCP controlled T38 fax relay call and when the gateway is configured for CA control T38. The output of the command **debug voip vtsp all** will give fax relay as “DISABLED”.

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

- 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.

- 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
```

- 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.

- CSCsy45838

  Symptoms: The **show ip ospf border-router** 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.

- 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.

- CSCsy49796

  Symptoms: HTTP redirect intermittently uses IP address instead of FQDN, even though an FQDN is configured in the WebVPN gateway.

  Conditions: The symptom is observed when the WebVPN gateway generates an HTTP redirect with an IP address when the HTTP Request from the client is not complete or split over multiple TCP packets.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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: There are two unrelated problems fixed by this bug:

  Problem 1: 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
```

  Problem 2: A nested crash might occur while generating a crashinfo. That means that this bug only helps the crashinfo to write properly. It does not fix the cause of the original crash, but will aid investigation.

  Conditions: Problem 1: This is only seen for memory corruption crashes when “exception region-size” is configured to a value that is not divisible by 4.

  Problem 2: BFD must be configured and sending hellos.

  Workaround: Problem 1: 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.

  Problem 2: Disable BFD.

- 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.

- 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.

- CSCsz02000

  Symptoms: Router reloads at “atm_update_bundle_counters”.

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsz08955

  Symptoms: This is a rarely occurring crash when ssg portmap and Transparent Auto Logon (TAL) are enabled together on a PPP session.

  Conditions: There is a timing issue that leads to a crash when ssg portmap and TAL are enabled together and when the PPP connection is terminated at the same time.

  Workaround: There is no workaround when both features are present in the configuration. It can be avoided when only one feature is present.

  Further Problem Description: When a session is being re-authenticated because of TAL and the PPP session is terminated at that time and also if it so happens that the connection has been idle for a while, then, because of timing issues in data structures, a situation might arise that can lead to a router crash.

  The solution will be available in the next release.

- 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.

- CSCsz16277

  Symptoms: A router crashes.

  Conditions: The symptom is observed when many (10 or more) SSLVPN clients are connected and router is under load (CPU>30%).

  Workaround: There is no workaround.

  Further Problem Description: Before the crash, typically the IO memory gets depleted. This can be verified with the **show memory statistics history** command.

- 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 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.

- CSCsz29542

  Symptoms: In the current implementation, “cwmp agent” identifies the WAN uplink if it has “cwmp wan default” configured on it. The WAN uplink interface differs, based on the router type used as a CPE. For the Cisco 871 router, WAN interface is FastEthernet 4 and for a Cisco 2811 router it is Fast Ethernet 0/0. This creates a problem in an SP-Managed service environment for the provisioning of CPEs (bulk deployment) using the TR-69 protocol.

  Conditions: The symptom is observed in an SP-Managed service environment for the provisioning of CPEs (bulk deployment) using the TR-69 protocol.

  Workaround: There is no work around.

- 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.

- CSCsz35204

  Symptoms: A Cisco 2821 router reloads sporadically, after enabling WebVPN using clientless web proxy method and extended access.

  Conditions: The symptom is observed with a Cisco 1841 router and a Cisco 2800 series router that is running Cisco IOS Release 12.4(24)T under moderate to heavy traffic.

  Workaround: There is no workaround.

- 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

- CSCsz39167

  Symptoms: If a tunnel is configured over the 880-3G cellular interface, traffic forwarding stops when the packet size is greater than the tunnel MTU.

  Conditions: The symptom is observed when a tunnel is configured over a cellular interface and running Cisco IOS Release 12.4(24)T.

  Workaround: Disable “ip cef”.

- 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/en/US/products/csa/cisco-sa-20100324-ldp.html

- 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/en/US/products/csa/cisco-sa-20100324-sip.html.

- 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

- 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.

- 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.

- 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.

- CSCsz62165

  Symptoms: Router crashes when a number of simultaneous PPPoE flow controlled sessions are cleared.

  Conditions: The symptom is observed when a series of seven or more routers are set up, and the sessions are brought up and down within 10 seconds.

  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:

  - Egress ACL configured on the interface.
  - A crypto map is applied to the same interface.

  - VSA is installed in the chassis.
  - 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100324-tcp.

- 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.

- 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".

- 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.

- 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/en/US/products/csa/cisco-sa-20100324-sip.html.

- 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.

- 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.

- 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.

- CSCta12296

  Symptoms: Group member router crashes.

  Conditions: Occurs when unicast re-keys are received frequently (TEK 300).

  Workaround: There is no workaround.

- CSCta16724

  Symptoms: Users with level 15 privilege and a “view” cannot do a Secure Copy (SCP).

  Conditions: The symptom is observed when a user with a “view” attempts to do an SCP.

  Workaround: Remove view.

- CSCta21892

  Symptoms: VPN client with certificates will fail IKE negotiations and show the following messages:

  ```
  Sev=Warning/2IKE/0xE300009B Failed to validate the payloads (MsgHandler:105)
  Sev=Warning/2IKE/0xE300009B Failed to process MM Msg 6 (NavigatorMM:570
  ```

  Conditions: The symptoms are observed with the following conditions:

  - VPN client connects to a router with certificates.
  - The router must be running Cisco IOS Release 12.4(24)T or later, or a version with the fix for CSCsv04325.

  Workaround: Use a Cisco IOS Release prior to 12.4(24)T.

  Further Problem Description: This issue is due to a change in Cisco IOS Release 12.4(24)T where the router will send the IKE phase 1 lifetime notification in MM6 (main mode 6th packet) and the client will reject it.

- 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.

- CSCta27331

  Symptoms: HSRP authentication applied to secondary addresses fails, generating the following syslog message:

```
%HSRP-4-BADAUTH: Bad authentication from 172.16.123.2, group 2, remote state Active
```

Conditions: The symptom is observed with HSRP authentication applied to secondary addresses. (HSRP authentication applied to primary addresses are unaffected.) It is seen with Cisco IOS Release 12.4(24)T and 12.2(33)SXI.

Workaround: Disable authentication on HSRP groups configured with secondary addresses.

- 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.

  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:

  ```
  Router# 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:

  ```
  certificates: Show certificates
  counters: Show PKI Counters
  crls: Show Certificate Revocation Lists
  server: Show 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.

- 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.

- 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.

- 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.

- 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.

- 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 RFC2833 to transport the DTMF signals, which causes problems with the Voicemail systems.

  Conditions: This symptom occurs when RTP header compression is enabled.

Workaround: There is no workaround.

Further Problem Description: The problem disappears if cRTP is disabled. The issue is seen with Class-Based cRTP configured and also with other cRTP configuration types.

- 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.

- 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.

- 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.

- CSCta91735

  Symptoms: Contact and Via ports are rewritten to 0.

  Conditions: The symptom is observed under the following conditions:

  - INVITE is sent from outside to inside.
  - Contact and Via headers in the SIP packet have a different port than the one specified as the outside port the configuration.

  Workaround: There is no workaround.

- CSCta96311

  Symptoms: Decrypted IPSec packets are not forwarded to the IVRF.

  Conditions: The symptom is observed with dual ISPs. It is seen when the primary default route is via a higher numbered interface and when crypto map is applied to both interfaces which go to the different ISPs.

  Workaround: Use the command **no ip route-cache cef** on the ingress interface of the incoming IPSec packet.

- CSCtb08032

  Symptoms: Unknown unicast packets are forwarded after bridging configuration is removed.

  Conditions: The symptom is observed after bridging is unconfigured on the l2 ports of the router.

  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 (a.k.a. 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.

- 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.

- CSCtb16459

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

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

  Workaround: There is no workaround.

- CSCtb25549

  Symptoms: Router crashes.

  Conditions: The symptom is observed with the following sequence:

  1. Use the command **debug condition username**.
  2. Bring up a VPDN session.
  3. Clear the VPDN tunnel on LAC.
  4. Remove the conditional debug.

  Workaround: There is no workaround.

- CSCtb26396

  Symptoms: HTTPS connections suddenly fail with the following error:

  ```
  //-1//HTTPC:/httpc_ssl_connect: EXIT err = -3, hs_try_count=1
  //394376//HTTPC:/httpc_process_ssl_connect_retry_timeout: SSL socket_connect failed
  fd(0)
  ```

  Conditions: The symptom is observed with CVP Standalone deployment running with HTTPS and with Cisco IOS Release 12.4(22)T1 or Release 12.4(24)T1.

  Workaround: Reload the gateway.

- 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.

- 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.

- CSCtb46556

  Symptoms: With a CJPA connected back-to-back to a Cisco 7200 series router with a NPE-G1 or NPE-G2, the NPE-G2 sometimes crashes when executing the command **clear int range multilink 1 10** and the NPE-G1 gives spurious access for the same command.

  Conditions: The symptoms are observed with a CJPA connected back-to-back to a Cisco 7200 series router with a NPE-G1 or NPE-G2 and when 14 multilinks are configured with two members each. Pagents are sending bi-directional traffic.

  Workaround: Do not perform commands across all interfaces using interface range. Perform the commands one-by-one, manually.

- 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.

- 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.
  ```

- CSCtb65151

  Symptoms: A device might crash with a bus error and the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

Conditions: The symptom is observed on a device that is running Cisco IOS Release 12.4(24)T1. Other releases may be affected (those running with the Common Classification Engine). The condition seems to be temporary and after a while it goes away.

Workaround: There is no workaround.

- 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.

- CSCtb79211

  Symptoms: A Cisco AS5400XM may process switch all traffic through interfaces. Other platforms may be affected.

  Conditions: The symptom is observed if you are running Cisco IOS Release 12.4(20)T or later and the interface is configured for netflow with one of the following feature sets:

  - c5400-ik9s-mz
  - c5400-ik9su2-mz
  - c5400-jk9su2_ivs-mz

  Workaround: Disable netflow.

- CSCtb95275

  Symptoms: Autocommands configured on VTY line or user-profile are not executing while logging through VTY.

  Conditions: The symptom is observed if the privilege level is not configured in the user profile.

  Workaround: Explicitly configure user privilege in the user profile.

- CSCtb95801

  Symptoms: In certain network setups, every five days the router hangs and the following error message is seen:

  ```
  SYS-2-BADSHARE: Bad refcount in datagram_done
  ```

  Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- CSCtb98080

  Symptoms: When you attempt to browse to a WebVPN portal you only see a blank page. The router does not send the browser a certificate and the portal login page is not displayed. The command **debug webvpn sdps** logs the following error message:

  ```
  WV-SDPS: Sev 4:sslvpn_tcp_read_notify(),line 1569:No to notify read: already queued[1]
  004549:
  ```

  Conditions: The symptom is observed when the SSLVPN process is waiting for an HTTP REQUEST from a client on the port configured using the **http-redirect <port no>** command but the process does not wake up. This can happen because of an unexpected IPC message to the SSLVPN process by another IOS process.

  Workaround: Remove **http-redirect** from the WebVPN gateway and reload the device.

- CSCtb98508

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

  Conditions: The symptom has been experienced on a Cisco 2851 router that is running Cisco IOS Release 12.4(20)T3 and when "callmonitor" is enabled.

  Workaround: There is no workaround.

- CSCtc04228

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

  Conditions: Using an earlier version of a Cisco IOS Release will enable the command.

  Workaround: After downgrading to a lower version where **mgcp behavior g729-variants static-pt** is not the default, configure **no mgcp behavior g729-variants static-pt** to remove the CLI.

- CSCtc04351

  Symptoms: The GM router might reload.

  Conditions: The symptoms is observed if the following conditions are met:

  1. Many VRFs are configured on the same GM, each belonging to an individual GETVPN group.
  2. All the VRFs are triggered to register with the KS at the same time.
  3. While #2 is happening, do a **clear cry gdoi** on the GM.

  Workaround: There is no workaround.

- CSCtc13664

  Symptoms: With an IPv6 Policy Based Routing (PBR) configuration, the route-map clause "set interface null0" may cause a router to crash.

  Conditions: The symptom is observed with IPv6 PBR. The trigger traffic is traceroute packets (ping packets will not cause the crash).

  Workaround: Configure "route-map" as [set interface loop0].

- CSCtc36826

  Symptoms: Unable to detect SIT and disconnect an FXO call.

  Conditions: The symptom is observed on an FXO port configured with "supervisory sit us immediate-release" or "supervisory sit us".

  Workaround: Configure "supervisory sit us all-tones".

Resolved Caveats—Cisco IOS Release 12.4(24)T1

Cisco IOS Release 12.4(24)T1 is a rebuild release for Cisco IOS Release 12.4(24)T. The caveats in this section are resolved in Cisco IOS Release 12.4(24)T1 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.

- 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.

- CSCsi69186

  Symptoms: Interface is reported by Optimized Edge Routing (OER) as being an invalid interface for sending an active probe.

  Conditions: Occurs on an Optimized Edge Routing (OER) border router with an external interface defined as a tunnel interface (mGRE).

  Workaround: There is no workaround.

- 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.

- CSCsj37160

  Symptoms: Cisco Express Forwarding (CEF) adjacency is going incomplete and local users are down. This may result in packet loss.

  Conditions: When the Peak rate on the ATM PVP is changed and “atm route-bridge ip” is configured on sub-interface, then adjacency goes to “incomplete” state.

  ```
  Config t
  interface ATM1/0
  atm pvp 11 3000 << change
  sh ip cef vrf Internet det | incl com
  Adj source: IP adj out of ATM1/0.44604, addr x.x.x.x (incomplete)
  ```
  Workaround: Clear adjanency or perform a **shut/no shut** on the ATM interface.

- 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.

- 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.

- 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.

- CSCsm75818

  Symptoms: Multicast data loss may be observed while changing the PIM mode of MDT-data groups in all core routers.

  Conditions: The symptom is observed while changing the PIM mode of MDT-data groups from “Sparse” to “SSM” or “SSM” to “Sparse” in all core routers in a Multicast Virtual Private Network (MVPN).

  Workaround: Using the command **clear ip mroute** *MDT-data group* will resolve the issue.

- 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.

- 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.

- CSCso90058

  Symptoms: MSFC crashes with Red Zone memory corruption.

  Conditions: This problem is seen when processing an Auto-RP packet and NAT is enabled.

  Workaround: There is no workaround.

- CSCsq40434

  Symptoms: Router crashes issuing "authentication network-eap eap_methods" under SSID in console line, when no SSID was issued from VTY line.

  Conditions: Occurs when using both console and VTY on a Cisco 3845 running Cisco IOS Release 12.4(19.18)T2 and the C3825-ADVSECURITYK9-M image.

  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.

- 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.

- CSCsr62645

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

  Conditions: Encountered during extended VLAN testing.

  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).

- CSCsr70963

  Symptoms: A Cisco 10000 PRE will reload unexpectedly when a radius server which is marked as dead is removed from the configuration during authentication of sessions.

  Conditions: The issue is seen when a RADIUS server is marked as dead. There are attempts to retry and access the server during its removal from the configuration.

  Workaround: There is no workaround.

- CSCsr94207

  Symptoms: The following bus error crash occurs:

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

  Conditions: "ntp broadcast destination" must be configured. Just having an NTP peer configured is not enough to trigger this crash.

  Workaround: There is no workaround.

- 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. The issue is seen only when frame-relay fragment and service-policy is part of map-class frame-relay configs

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

- 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.

- 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.

- 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.

- 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.

- 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.

- 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 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.

- CSCsv68584

  Symptoms: Router crashed when 100 PPPoE sessions are created with policy protocol L2TP.

  Conditions: This symptom occurs while PPPoE sessions are created.

  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.

- CSCsv81751

  Symptoms: Cisco 7200 G2 router crashes when changing configuration of serial interfaces from PPP to SDLC and back to PPP, while running traffic.

  Conditions: This is observed on a T3 link with 56 channel groups configured on a WAN aggregation device. All the serial interfaces have service-policy configured.

  Workaround: Remove the service-policy before changing the encapsulation to SDLC.

- 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.

- 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.

- 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 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.

- 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.

- 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.

- 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.

- CSCsw24826

  Symptoms: Cisco router may crash pointing to OSPF code because of low memory access.

  Conditions: Crash is specific to the following scenario:

  1. Neighbor router performs IETF NSF restart.
  2. Software interface between routers is removed from configuration when NSF restart is undergoing, when grace LSA is present in the database of the helper router.
  3. Helper router will crash 1 hour later during max-age procedure for grace LSA. Reason is that grace LSA is associated with interface, but that interface does not exist any more.

  Workaround: If configuration changes need to be done during network changes, the following applies:

  1. Shutdown OSPF interface
  2. Check **show ip ospf da**. Can you see type-9?
     - NO => good, remove interface
     - YES => ’no shutdown’ interface, wait for neighbor going FULL (type-9 will be flushed during sync)
  3. Repeat Step 1.

- 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.

- 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.

- CSCsw49464

  Symptoms: The router processes SSLVPN_PROCESS, and pool manager may hold most of a Cisco 1811 router's memory, which may affect the routers capability to process SSLVPN traffic.

  Conditions: This happens after many users log in to a router acting as an SSLVPN gateway.

  Workaround: Disable the on-board crypto engine with the **no crypto engine onboard 0** command

- CSCsw50811

  Symptoms: When **ipv6 mld static-group** is configured on a non-DF interface, IPv6 Protocol Independent Multicast (PIM) topology table is not seen after doing **shut/no shut** on non-DF interface.

  Conditions: This happens with a Cisco 7200 router that is running Cisco IOS Release 12.4(24)T.

  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.

- CSCsw65929

  Symptoms: A crash may occur upon disabling ccm-manager fallback.

  Conditions: The symptom is observed when disabling and enabling MGCP application and ccm-manager fallback in quick succession.

  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.

- 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.

- CSCsw66151

  Symptoms: Dynamic Multipoint VPN (DMVPN) version 6 hub crashes.

  Conditions: Occurs when traffic is passed from the router behind the spoke to another device.

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.

- CSCsw68626

  Symptoms: Router crashed after executing the **no server name** command.

  Conditions: Occurs while removing the configured server name from a AAA server group on a Cisco 7200 router.

  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.

- CSCsw72132

  Symptoms: The router crashes when bringing up large number of sessions.

  Conditions: Occurs when 500 sessions have to be cleared.

  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.

- 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: 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.

- 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.

- 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.

- 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.

- CSCsw93187

  Symptoms: Ingress MPLS EXP marking malfunctioning on Multilink Frame Relay (MFR) Interface.

  Conditions: Occurs with MFR interface on Cisco 7200 router.

  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.

- CSCsw95670

  Symptoms: With Ethernet over MPLS configured in VLAN interface, End-to-End connectivity is broken between CE routers.

  Conditions: The issue is seen on router loaded with an internal build of 12.2(33)SR.

  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.

- 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-tunnel** 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.

- CSCsx06534

  Symptoms: Cisco IOS certificate server crashes while shadow certificate takes over after a manual reload.

  Conditions: This seems to only happen under test conditions where the system clock is modified. There may be a rare instance where this could happen without the clock being modified.

  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.

- CSCsx09110

  Symptoms: Cisco voice gateway may be unable to establish IPSec tunnel to a Cisco Call Manager (CCM)

  Conditions: Occurs when the gateway is running Cisco IOS Release 12.4(23.15)T3 or later.

  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.

- CSCsx10140

  Recent research (1) has shown that it is possible to cause BGP sessions to remotely reset by injecting invalid data, specifically AS_CONFED_SEQUENCE data, into the AS4_PATH attribute provided to store 4-byte ASN paths. Since AS4_PATH is an optional transitive attribute, the invalid data will be transited through many intermediate ASes which will not examine the content. For this bug to be triggered, an operator does not have to be actively using 4-byte AS support.

The root cause of this problem is the Cisco implementation of RFC 4893 (4-byte ASN support) - this RFC states that AS_CONFED_SEQUENCE data in the AS4_PATH attribute is invalid. However, it does not explicitly state what to do if such invalid data is received, so the Cisco implementing of this RFC sends a BGP NOTIFICATION message to the peer and the BGP session is terminated.

RFC 4893 is in the process of getting updated to avoid this problem, and the fix for this bug implements the proposed change. The proposed change is as follows:

"To prevent the possible propagation of confederation path segments outside of a confederation, the path segment types AS_CONFED_SEQUENCE and AS_CONFED_SET [RFC5065] are declared invalid for the AS4_PATH attribute. A NEW BGP speaker MUST NOT send these path segment types in the AS4_PATH attribute of an UPDATE message. A NEW BGP speaker that receives these path segment types in the AS4_PATH attribute of an UPDATE message MUST discard these path segments, adjust the relevant attribute fields accordingly, and continue processing the UPDATE message."

The only affected version of Cisco IOS that supports RFC 4893 is 12.0(32)S12, released in December 2008.

(1) For more information please visit:

http://www.merit.edu/mail.archives/nanog/msg14345.html

- CSCsx11776

  Symptoms: Executing the commands **show ip bgp version recent 1** or **show ip bgp version 1** from EXEC mode may cause the device to crash.

  Conditions: The symptom is observed in affected images that have support for BGP.

  Workaround: Use AAA command authorization to prevent the use of these commands.

  Further Problem Description: 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.

- CSCsx15038

  Symptoms: NVgen issue occurs 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 reflected under **show run** output.

  Workaround: Do not configure as a whole with "policy cir" and "exceed command". Configure as individual commands.

- 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.

- 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.

- 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.

- CSCsx20984

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

  Conditions: Unknown at this time.

  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.

- 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.

- CSCsx24996

  Symptoms: Removing tunnel configuration can cause the router to crash.

  Conditions: Occurs when the tunnel is removed while QoS is active on that tunnel.

  Workaround: Stop traffic to the tunnel, remove QoS and then delete the tunnel configuration.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-sip.

- 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.

- 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.

- CSCsx32283

  Symptoms: Router is crashes.

  Conditions: Occurs because of malformed LDAP packet.

  Workaround: There is no workaround.

- 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 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.

- CSCsx41059

  Symptoms: Cisco 7200 router crashes when **ip sla ethernet probe** is configured.

  Conditions: Occurs when the following commands are entered:

  cns config notify diff interval 5

  ip sla ethernet echo oper

  Workaround: Do not configure **cns config notify diff interval 5** when configuring **ip sla opers**.

- 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.

- CSCsx41519

  Symptoms: Cisco 7200 router crashes while removing configuration for internal testing.

Conditions: Occurs on a router running an internal build of Cisco IOS Release 12.4T.

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**.

- CSCsx44172

  Symptoms: A privilege 15 user being authorized against a TACACS server can issue certain commands containing the arguments "full" or "brief" although these commands are disallowed in the TACACS server. For instance:

  - show running-config brief

  - show running-config full

  Conditions: When running TACACS debugs when the commands are executed, we can see that the privilege level is set to 0 for these commands, although the correct level should be 15. The router is configured with the following:

  aaa authorization config-commands

  aaa authorization exec default group tacacs+ if-authenticated

  aaa authorization commands 0 default none

  aaa authorization commands 1 default group tacacs+ if-authenticated

  aaa authorization commands 15 default group tacacs+ if-authenticated

  Workaround: There is no workaround.

- 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 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.

- CSCsx46297

  Symptoms: Easy VPN across Dynamic Virtual Tunnel Interface (DVTI) malfunctions after re-key.

  Conditions: Happen only across DVTI. This is not seen with static interfaces.

Workaround: There is no workaround.

- 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.

- 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.

- CSCsx48939

  Symptoms: Configuring police "CIR" displays as rate under **show policy-map**.

  Conditions: Above symptom is seen in Cisco routers running Cisco IOS Release 12.4(23.15)T3.

  Workaround: There is no workaround.

- CSCsx49358

  Symptoms: Cisco router may face ping failure between provider and customer networks.

  Conditions: Occurs on routers running Cisco IOS Release 12.4(23.15)T3.

  Workaround: There is no workaround.

- 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.

- CSCsx49881

  Symptoms: Bandwidth is not allocated correctly when UBR/ABR value of 5000 is used. ATM PVC initially comes up with 5000 BPS but does not readjust correctly

  Conditions: This symptom is observed on a Cisco router ATM IMA interface when "vc-class" is used. It works fine for 1000.

Workaround: There is no workaround.

- 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: 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.

- CSCsx51674

  Symptoms: Agent entry is not seen.

  Conditions: Occurs on a roaming interface that is configured for Collocated Care-of Address (CCoA). The mobile router will not see it as a usable interface.

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

- 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.

- CSCsx55240

  Symptoms: Router crash seen at “html_config_command”.

  Conditions: This issue is observed on a Cisco 7200 router running Cisco IOS Release 12.4(24.2)T.

  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 transitting 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 pattern.

- CSCsx57110

  Symptoms: H.324 video calls fail.

  Conditions: Occurs when calls go from H.323 leg to SIP leg. Call becomes audio only.

  Workaround: Add the following command to the VoIP dial-peer:

  voice-class sip calltype-video

- 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.)

- CSCsx58889

  Symptoms: Calls fail intermittently with cause “47: no resource available” error.

  Conditions: Occurs when router is under load test.

  Workaround: There is no workaround.

- 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.

- CSCsx59309

  Symptoms: Cisco IOS routers crash when filter style is changed from fixed filter (FF) to wild card filter (WF).

Conditions: Occurs when FF style reservation is installed on an interface and is then modified to WF style without first removing the FF style reservation.

Workaround: Remove FF style reservation before configuring for WF style reservation.

- 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.

- CSCsx61138

  Symptoms: Bindings are not cleared after the **clear ip mobile binding** *ip address*.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(23.15).

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-tunnels.

- 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.

- 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.

- 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.

- 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.

- CSCsy07953

  Symptoms: Any attempt to copy a file from a router to an FTP server will fail. The FTP error is "No such file or directory".

  Conditions: This is only a problem with FTP and only when transferring to an FTP server. Transfers from an FTP server work as expected.

  Workaround: Use a different file transfer protocol, such as TFTP.

- 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.

- 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).

- CSCsy14244

  Symptoms: Video call between two Cisco Unified Video Advantage endpoints results in one-way audio and no video.

  Conditions: Occurs when call passes through Cisco Unified Border Element (CUBE).

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy

- 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 router 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: Occurs when the device has **debug crypto isakmp** enabled.

  Workaround: Remove this debug command.

- 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.

- 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.

- 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.

- 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.

- CSCsy22825

  Symptoms: Chunk leak is seen whenever one PPPoE session is cleared.

  Conditions: Occurs only when one session is cleared.

  Workaround: There is no workaround.

- 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).

- 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.

- CSCsy45371

  Symptoms: The **clear ip nat tr *** commandremoves 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-acl.

- 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.

- 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.

- 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: 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.

- 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.

- CSCsz00890

  Symptoms: Cisco 7200 router crashes.

  Conditions: Occurs when Distributed LFI over ATM (dLFIoATM) is configured on a Cisco 7200 and a QoS policy is attached.

  Workaround: There is no workaround.

- CSCsz05783

  Symptoms: Voice/SIP (ef) packets are not marking in the ingress/egress when NAT is enabled on the interface.

  Conditions: Occurs when NAT is enabled.

  Workaround: Remove NAT from the configuration.

- 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.

  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.

- CSCsz21577

  Symptoms: SIP-NAT SBC does not properly preserve the Contact Header for outside-to-inside translations.

  Outside Packet:

  ```
  Contact: "EMTAlinea1"<sip:1188800099@192.168.15.10:1032;transport=udp>;expires=1674
  ```

  Inside Packet:

  ```
  Contact: "EMTAlinea1"<sip:1188800099@10.0.2.101:5060;expires=60
  ```

  Conditions: Only seen on outside-to-inside translations when using the registration-throttle feature.

  Workaround: There is no workaround.

- 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: 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-h323.

- 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.

- 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.

- 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.

- 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.

- CSCsz55293

  Symptoms: A remote third-party device is resetting the IPv6 BGP session with a Cisco 12000 router.

  Conditions: BGP is exchanging only IPv6 capability with the remote EBGP peer, but IPv4 capability will be enabled by default. The remote EBGP peer is sending only IPv6 capability, and we should advertise only IPv6 prefixes because that is the capability negotiated. We are wrongly marking IPv4 capability as negotiated and advertising IPv4 prefixes, and the remote neighbor is resetting the session because IPv4 capability is not negotiated at the peer end.

  Workaround: Configure a route map to deny all IPv4 prefixes, and apply it as follows:

  ```
  Route-map deny-ipv4 deny 10
  Router bgp <asnum>
  address-family ipv4
  Neighbor <IPv6Address> activate
  Neighbor <IPv6Address> route-map <deny-ipv4> out
  ```
- 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.
- 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.

- 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: Power cycle the router to recover from this hang state. The router will then boot with the upgraded ROMmon.

- 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.

- 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.

- 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.

- 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.

- CSCta03167

  Symptoms: Cisco router crashes.

  Conditions: Occurs when you change your present working directory to a directory where an images is located. Using the **secure boot-image** command to secure the image causes the crash.

  Workaround: There is no workaround.

- CSCta04391

  Symptoms: Router with dynamic NAT configuration crashes after deleting **ip nat inside source list**.

  Conditions: Router crashes only when there is unicast and multicast traffic and the following sequence of steps occurs:

  1. **clear ip nat translation *** or **clear ip nat translation forced**.
  2. no ip nat inside source list access-list-number pool pool-name

  Workaround: Delete **ip nat inside source list** without clearing NAT translations.

- CSCta80298

  Symptoms: The SFP ports are shown in the ENTITY MIB even though the SFPs are not inserted.

  Conditions:

  The symptom is observed with PA-POS-2OC3 module in Cisco7200 for Cisco IOS Release 12.4(24)T1.

  Workaround: There is no workaround.

Further Problem Description:

With the ANA model, the device operates properly the first time when the SFP is inserted (SFP module ==> SFP container ==> port). But once the SFP is pulled out, the port incorrectly goes under the container. When you insert the SFP, the same port comes under the module. Since ANA will not delete the port, the same port gets two parents which ANA will not accept. With this fix, the ENTITY MIB will not populate the PORT entry unless XCVR exists.

Open Caveats—Cisco IOS Release 12.4(24)T

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(24)T. All the caveats listed in this section are open in Cisco IOS Release 12.4(24)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Miscellaneous

- CSCsk89671

  Symptoms: When a simple shaping policy is applied on a Dynamic Multipoint VPN (DMVPN) tunnel, and multicast traffic is forwarded over the tunnel, shaping functionality is broken.

  Conditions: Shaping functionality works for unicast traffic. The issue is seen only with multicast traffic.

  Workaround: There is no workaround.

- CSCsm53260

  Symptoms: TCP may exhibit some unexpired managed timers. The TCP retransmission timer for a given TCB in **show tcp** may be past due.

  Conditions: This is a rare situation.

  Workaround: There is no workaround.

- 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.

- CSCso87768

  Symptoms: Cisco 877 and Cisco 878 routers suffer from flapping ATM interfaces.

  Conditions: Observed with Cisco 877 and Cisco 878 routers configured for ADSL2+ training to Nokia D500 DSLAM.

  Workaround: There is no workaround.

- CSCsq14998

  Symptoms: GPRS Gateway Support Node (GGSN) router crashed while doing stress testing after 30 minutes using iSCSI. Traceback pointed to parse_radius_response.

  Conditions: Router configured for 120K IP packet data protocol (PDP) and sends bidirectional IMIX traffic at 99 kpps. When call detail records (CDRs) are written to iSCSI, GGSN uses 99% CPU.

  Workaround: There is no workaround.

- CSCsq47730

  Symptoms: Router displays the following error message, then freezes:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle
  ```
  A reload is required to recover.

  Conditions: Occurs on a Cisco 1803 running Cisco IOS Release 12.4(6)T7.

  Workaround: There is no workaround.

- CSCsq75772

  Symptoms: Classification failed on virtual interface.

  Conditions: Occurred on a Cisco 7200 router running Cisco IOS Release 12.4(15)T06.

  Workaround: There is no workaround.

- CSCsr01717

  Symptoms: GPRS: Gateway Support Node (GGSN) continually reboots.

  Conditions: Occurs when configured for Redundancy Facility (RF) inter-device.

  Workaround: There is no workaround.

- 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 for after use of TCL [connection create] command.

  Conditions: Occurs with TCL application running on Cisco IOS Release 12.4(15)T6 and 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.

- CSCsr99642

  Symptoms: HWIC-2SHDSL is not recognized after warm reload of Cisco 2821. Unknown VWIC messages are seen on console.

  Conditions: Occurs on a Cisco 2821 with HWIC-2SHDSL module. Enabling warm reboot and issuing **reload warm flash:iosimage.bin** causes this problem.

  Workaround: Cold reboot the router. Do not use warm reload feature.

- CSCsu05186

  Symptoms: The following command do not work:

  dot1x timeout supp-response dot1x timeout reauth-period

  Conditions: Occurs when configuring wireless on a Cisco 871 router.

  Workaround: There is no workaround.

- CSCsu25644

  Symptoms: Router crashes after the removing the tunnel source interface before entering the **no interface tunnel** command.

  Conditions: Occurred during Dynamic Multipoint VPN (DMVPN) testing when there are more than 150 DMVPN tunnels.

  Workaround: There is no workaround.

- CSCsu42583

  Symptoms: Any image or large file is corrupted when copied to disk. The following error message is displayed:

  ```
  Error reading disk2:<filename> (Clusterchain broken on file)
  ```

  Conditions: Happens only when a compact flash card is present.

  Workaround: Replace the compact flash card with another model, one that is supported by Cisco.

- CSCsu49189

  Symptoms: Frame-Relay fragment output not seen when modifying the attached map-class.

  Conditions: Occurs on a Cisco 7200 router.

  Workaround: Detach and attach Frame-Relay fragment.

- 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.

- CSCsu86004

  Symptoms: Cisco Unified Border Element (CUBE) crashed.

  Conditions: This occurs when remote SCCP phone registration message passes through ZBFW/CUBE with “ip virtual-reassembly” configured under the interfaces of the private and public zones.

  Workaround: There is no workaround.

- CSCsv09180

  Symptoms: Router will crash upon removing service policy and DLCI associated with a frame-relay interface.

  Conditions: The router if the following steps are performed in the order given:

  1. Configure frame-relay encapsulation on serial interface and assign IP address.

  2. Configure header compression on it through policy-map using the **service-policy output** command.

  3. Associate the interface with DLCI using the **frame-relay interface-dlci** command.

  4. Configure the remote router in a similar fashion and ensure both interfaces ping each other.

  5. Remove the policy-map on local router using the **no service-policy output** command.

  6. Remove the DLCI associated using the **no frame-relay interface-dlci** command. This causes the router to crash.

  Workaround: There is no workaround.

- CSCsv63265

Symptoms: A performance degradation of 7% occurs for Cisco 2801 with security configured.

Conditions: Problem is seen when utilizing 75% CPU and using 3DES IPSec transform with SHA authentication and 100 tunnels.

Workaround: There is no workaround.

- CSCsv65147

  Symptoms: Protected Extensible Authentication Protocol (PEAP) with secure token not working.

  Configure Occurs on a Cisco 800 series router and a client using PEAP with secure token.

  Workaround: There is no workaround.

- CSCsv65309

  Symptoms: A call through a Cisco Unified Border Element (CUBE) does not establish two-way audio. The call may drop.

  Conditions: Occurs if the endpoint to which 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.

  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.

- CSCsv69460

  Symptoms: Ping failed between two customer routers. Customer routers are connected through two PE routers, and PE routers are connected to each other by ATM point-to-point link.

  Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(15)T8

  Workaround: There is no workaround.

- CSCsv76947

  Symptoms: Cisco router with HWIC-2CE1T1-PRI may unexpectedly reload when the **show controllers** command is executed at the same time one of the channels on the card goes down.

  Conditions: Show controllers must be executed at the same time the channel goes down.

  Workaround: There is no workaround.

- CSCsv82317

  Symptoms: WIC-4SHDSL: Inconsistency in train up with m-pair Annex interchange.

  Conditions: With the HWIC-4SHDSL scenario, when we create mpair DSL group link, it may fail to train with default B annex. Sometimes with annex B trains up, but when we interchange to annex A, it fails to train up. Also sometimes when we issue **shut/no shut** on CPE/CO side, it fails to train up.

  Workaround: Swapping the termination mode and reloading both the routers may bring up the line successfully. It can be repeated multiple times if controller line does not train properly in the back-to-back setup. This workaround may not be suitable in a customer environment.

- 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.

- 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.

- CSCsv93421

  Symptoms: Group member crashed when downloading a large number of access-lists from the key Server.

  Conditions: This crash was seen when the key server was configured with 100 access-lists that permit traffic from 50 hosts on either sides of the group members.

  Workaround: Configure a smaller number of ACLs.

- CSCsv96409

  Symptoms: Router crashes VFR is enabled and CEF is turned off.

  Workaround: Disable VFR using the **no ip virtual reassembly** command.

  Workaround: There is no workaround.

- CSCsv96630

  Symptoms: Memory leak occurs on ISR transcoder router.

  Conditions: Occurs when the secure option is added to a transcoder configuration in a topology with a Cisco Unified Communication Manager 7.1.

  Workaround: Remove the secure configuration from the transcoder.

- CSCsv97424

  Symptoms: Router crashes due to memory corruption in the I/O pool. In all of the crashes previous block pointer is corrupted.

  Conditions: Observed in a Cisco 2811 running Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsw14688

  Symptoms: High CPU utilization is noticed for PPP events, causing increased number of PPP session flaps.

  Conditions: The problem is noticed on Cisco 7206VXR with NPE-G1 processor running Cisco IOS Release 12.4(15)T5.

  Workaround: There is no workaround.

- CSCsw20194

  Symptoms: Tunnels flapping. Traffic fails (all counters show “0”) even when the tunnels are up.

  Conditions: Occurs when a service-policy is attached to a PVC.

Workaround: Delete the service-policy, then wait for about 30 seconds. The tunnels will recover and traffic can resume, then add the service-policy back.

- CSCsw27984

  Symptoms: A Cisco 7200 router running Cisco IOS Release 12.4(20)T1 reboots with a bus error.

  Conditions: The router is configured with ios-firewall. The crash was observed one time only.

  Workaround: There is no workaround.

- CSCsw32795

  Symptoms: Key server crashes during configuration.

  Conditions: Occurs when key server is configured with two or more GDOI groups.

  Workaround: There is no workaround.

- CSCsw34941

  Symptoms: Router crashes while performing online insertion and removal (OIR) of two NM-1A-OC3-POM cards at the same time.

  Conditions: Occurs on a Cisco 3845 with two NM-1A-OC3-POM installed at slots 2 and 4. When both are removed, the router crashes sometimes.

  Workaround: Do OIR one by one.

Resolved Caveats—Cisco IOS Release 12.4(24)T

This section describes possibly unexpected behavior by Cisco IOS Release 12.4(24)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.

- CSCek75694

  Symptoms: A router 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.

- 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.

- 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.

- 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 command **crypto key zeroize rsa** 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/warp/public/707/confaccesslists.html

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsm27071

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

- 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.

- 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.

- CSCsm73364

  Symptoms: The router will crash if the routing instance has been removed and an instance-specific command is issued (e.g. shutdown, maxpaths, split horizon etc).

  Conditions: The symptom is observed when removing an instance from either console or VTY while another console or VTY is still in router mode.

  Workaround: Exit and re-enter router mode before issuing any instance- specific commands.

- CSCsm97220

  Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip

- CSCso24954

  Symptoms: A policy with unsupported queuing features is allowed to attach to sessions. It may cause potential issues that require a reload to recover.

  Conditions: There are no specific conditions required for this issue.

  Workaround: There is no workaround.

- CSCso49388

  Symptoms: Router crashes on attaching the policy which contains “queue-limit” configuration in the input direction of any interface.

  Conditions: Occurs on Cisco 7200 routers with NPEG1 processor and Cisco 7301 routers.

  Workaround: There is no workaround.

- 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.

- 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 12.4.15T4.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCsq44761

Symptoms: Different crashes are seen in the nhrpSnmpCompareNodes routine.

Conditions: The symptom is observed in the nhrpSnmpCompareNodes routine while configuring IPv6.

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.

- 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-cme.

- CSCsq73501

  Symptoms: Unable to create sessions and ACLs.

  Conditions: The symptom is observed when testing with DACL.

  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 the **multi-path** command on Cisco IOS Release 12.4(9)T.

  Workaround: There is no workaround.

- CSCsr18173

  Symptoms: 1. If dampening is enabled on a router, and identical updates of a IPv4 prefix carrying label information are received, these updates are not treated as identical and dampening penalty is set for the route. 2. If dampening is enabled on a router, and identical updates of a IPv4 multicast prefix are received, these updates are not treated as identical and dampening penalty is set for the route.

  Conditions: The symptom is observed when dampening is enabled and: 1. Identical updates of a IPv4 prefix are received. The updates should be carrying MPLS Label information; or 2. Identical updates of a IPv4-multicast prefix are received.

  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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-ios-fw

- CSCsr21842

  Symptoms: On a Cisco 7200 series router that has a crypto map protecting GRE tunnel traffic, putting an inbound ACL to drop the decrypted, GRE- decapsulated IP traffic may not work. The traffic is not dropped as expected and there is no hit count on ACL/ACE (although permit ACE still works properly and receives hit counts).

  Conditions: The symptoms are observed with the following conditions: 1. On a Cisco 7200 series router with K9 images. 2. Where a crypto map is applied on a physical interface protecting GRE tunneling traffic (47 host2host) 3. When “deny inbound ACL” is configured on the tunnel interface to drop the cleartext (the traffic will not be dropped as expected). 4. It occurs with certain configuration sequences, such as configure tunnel and crypto map. (If you bring up IPSec SA, then apply inbound ACL to the tunnel interface, then save the configuration at the start-up configuration and boot from there, the issue may not show up.) 5. This only affects inbound ACLs. Outbound ACLs are not affected

  Workaround: Use an inbound crypto map ACL (ipsec-dACL) instead of a inbound ACL on tunnel in this senario. Inbound crypto map ACL sees the decrypted GRE packets, and it can drop the traffic properly. For example:

  ```
  router#sh cry map Crypto Map "testtag" 10 ipsec-isakmp Peer = 10.0.0.8 Extended IP
  access list 101 access-list 101 permit gre host 10.0.0.9 host 10.0.0.8 Extended IP
  access check IN list imacl access-list imacl permit ahp any any access-list imacl
  permit esp any any access-list imacl deny gre any any access-list imacl permit ip any
  any Current peer: 10.0.0.8 Security association lifetime: 4608000 kilobytes/3600
  seconds PFS (Y/N): N Transform sets={ proposal1: { ah-sha-hmac } , { esp-3des
  esp-sha-hmac } , } Interfaces using crypto map testtag: GigabitEthernet0/1
  ```

  Alternate workaround: Turn off CEF switching and use process switching.

- 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.

- CSCsr27734

  Symptoms: The standby router crashes.

  Conditions: This symptom is observed when a service-policy map is removed from a VC.

  Workaround: There is no workaround.

- CSCsr36971

Symptoms: On a chassis with large number of v4 and v6 VRFs and multicast, a memory leak may be seen for the PIM process.

Conditions: The symptom is observed when running ION. There is no multicast traffic flowing but IPv4 and IPv6 VPN traffic is flowing.

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 "no keepalive" on the interface that is down.

- 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.

- 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.

- 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.

- CSCsr55922

  Symptoms: The EIGRP IPv6 process may incorrectly select a router-ID from the 127.0.0.0 address range.

  Symptoms: The same router-ID may be selected on two separate Cisco routers configured for EIGRP IPv6. External prefixes advertised by one of the EIGRPv6 routers will be ignored by the receiving EIGRPv6 router due to the fact the routerID contained in the external data portion of the prefix matches the receiving routerID; a loop prevention method.

Workaround: Manually configure a router-ID under the EIGRP IPv6 process with **router-id**<*address*> command.

- CSCsr55990

  Symptoms: HSRP virtual MAC is dynamic instead of static on a Cisco 7600 after a reload.

  Conditions: HSRP is configured under a routed vlan-based pseudowire:

  interface Vlan X ip address 10.0.0.1 255.255.255.0 standby 1 ip 10.0.0.254 xconnect x.y.z.w encapsulation mpls

  Occurs when fast millisecond HSRP timers are used, and an HSRP interface delay is not configured.

  Workaround: Perform a **shut/no shut** on the interface "vlan X". Or, as a preventive action, configure **standby delay minimum 60** on the interfaces. Testing has shown that after a reboot the entry is installed correctly in the PFC/DFC.

- 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.

- CSCsr64777

  Symptoms: A router crashes because of a block overrun (overwriting the memory block).

  Conditions: This symptom is observed only when NetFlow version 5 is used.

  Workaround: NetFlow version 9 could be used for exporting.

- 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.

- 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.

- CSCsr85093

  Symptoms: SSH connection fails to establish after SSO with the following debug message on client side:

  SSH2 CLIENT 0: RSA signature verification failed, status 524

  Conditions: This symptom occurs when a new RSA key is generated. The SSH server key is not updated on the standby. The **show ip ssh** command on the standby will show that SSH is enabled, but the SSH connection will fail to establish.

  Workaround: Regenerate RSA key on the new active after SSO.

- 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.

- CSCsr93969

  Symptoms: Autoinstall requires user to respond “No” to initial configuration dialog before proceeding with autoinstall process.

  Conditions: The symptom is observed whenever the user does a “write erase” and reload to invoke autoinstall.

  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.

- CSCsr96468

  Symptoms: The following may be seen on a Catalyst 3750 if an HSRP version 2 group is configured after an HSRP version 1 group:

  Vlan5 - Group 300 (version 2) State is Init (virtual MAC reservation failed)

  The correct behavior is for the HSRP version 2 group to be rejected since the Catalyst 3750 only supports MAC addresses for one HSRP version at any one time.

  Conditions: This only affects the catalyst 3750 platform.

  Workaround: Remove the HSRP version 2 group.

- 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.

- CSCsr97030

  Symptoms: Service policy is missing from the running-configuration after a device is reloaded.

  Conditions: The symptom is observed when the service policy contains a “police rate percent” that is 13% or less, and is applied to an MLPPP interface. It is observed with Cisco IOS Release 12.4(8c) and Release 12.4T.

Workaround: Use any one of the following: 1. Re-apply service-policy each time after rebooting. 2. Change service policy to use "police rate XXXX bps". 3. Configure bandwidth XXXX on the MLPPP interface. 4. Change service policy to use more than 13% for the policing.

- CSCsr97753

  Symptoms: Pinging an interface fails.

  Conditions: Occurs when unconfiguring xconnect on the interface.

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

- 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.

- 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

- 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 command **as-override** 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ctcp.

  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

- 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** 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

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-ntp

- 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.

- CSCsu27109

  Symptoms: When stateful switchover (SSO) is performed on a Cisco 7600, MPLS label allocation fails.

  Conditions: Issues are seen on Cisco 7600 router. Occurs after performing the SSO. Also seeing CPU usage above 95% for 10-15 minutes.

  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.

- 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.

- CSCsu31444

  *Crash observed after configuring a policy-map

- 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.

- 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.

- 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 outbound on the serial interface. This symptom 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 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.

  - Issue is seen with F/G annex; the issue is not seen with A/B annex.
  - CO side link goes down, but the CPE comes up.

  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.

- 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.

- 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 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.

- 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.

- CSCsu38842

  Symptoms: Memory leak from "HQF: hqf feature(s) data" is observed.

  Conditions: Occurs after configuring class-based WRED and reconfigure fair-queue for class-default.

Workaround: There is no workaround.

- CSCsu40234

  Symptoms: Traffic may fail with VSA and time-based anti-replay.

  Conditions: The symptom is observed when GetVPN and time-based anti-replay are configured with the VSA module.

  Workaround: Remove time-based anti-replay from the GetVPN Key Server configuration.

- CSCsu41968

  Symptoms: On a Cisco 7500 with an HA setup, the "show controller t3" command is showing framing as M23 on the active and as C-bit on the standby. So the "loopback remote" configuration is rejected on the active and is accepted on the standby.

  Conditions: This symptom is observed when the "show controller t3 1/1/0" command is issued.

  Workaround: There is no workaround.

  Further Problem Description: Because of the framing mismatch, the standby might crash due to sync issues.

- 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.

- 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.

- 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.

- CSCsu46871

  Symptoms: Unable to attach service policy to VT when bandwidth is configured in class default.

  Conditions: Occurs when DLFI over ATM is configured while trying to attach service policy to VT when bandwidth is configured in class default.

  Workaround: Configure bandwidth in user defined class and attach to VT.

- 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-acl.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-acl.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-ntp

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-acl.

- CSCek48205

  Symptoms: The output counters for a Multilink Frame Relay (MFR) bundle interface may not be updated correctly.

  Conditions: Occurs after the same interface is deleted and recreated.

  Workaround: There is no workaround.

- CSCsd80349

  Symptoms: In a MPLS Traffic Engineering Fast Reroute environment, if the line protocol on the protected link goes down due to mismatched keep-alives on the link (or too many collisions), the forwarding plane does not switch traffic for protected label switched paths (LSP) to their respective backups.

  Conditions: Occur under the following scenario:

  - A Cisco router running a Cisco IOS Release 12.2S
  - Router acting as a Point of Local Repair (PLR) for MPLS Traffic Engineering Tunnels that request Fast Reroute protection
  - Mismatched keep-alives or excessive collisions on the protected link.

  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.

- CSCsk26651

  Symptoms: A router crashes when configuring auto qos on an ATM subinterface. The following error message is produced: "%SYS-6-STACKLOW: Stack for process Exec running low"

  Conditions: The symptom occurs when AutoQoS Discovery is enabled for untrust mode, and also when AutoQoS Discovery is enabled for trusted DSCP.

  Workaround: There is no workaround.

- CSCsk52143

  Symptoms: On a Cisco Catalyst 6509, a WS-SUP32-GE-3B, a Cisco 7600-SIP-400, a SPA-1XOC12-POS, a Cisco 7600-SSC-400 and a SPA-IPSEC-2G, configuring a hierarchical policy with multiple parent shapers (in user defined classes) and child queuers results in the **police cir percent** command (which MUST be used with the "priority" CLI on a SIP-400 in SRA to avoid PQ monopolization) policing data in the parent-policy in accordance with the following formula: ("police cir percent") * (LOWEST "shape average") instead of the expected behavior: ("police cir percent") * ("shape average") For example, in this policy: policy-map cbwfq-ip class tunnel13601 shape average 80000000 service-policy cbwfq-sip class tunnel13603 shape average 20000000 service-policy cbwfq-sip The policer in the child policy-map (below) will police both classes tunnel13601 AND tunnel13603 to 66% of 20000000 (when it should police class tunnel13601 to 66% of 80000000 and class tunnel13603 to 66% of 20000000): policy-map cbwfq-sip class out-voice priority police cir percent 66 conform-action transmit exceed-action drop violate-action drop class out-streaming bandwidth remaining percent 15 class out-time-sensitive bandwidth remaining percent 10 class out-troubleshooting bandwidth remaining percent 2 class out-viruscontrol bandwidth remaining percent 1 queue-limit 128 packets class class-default bandwidth remaining percent 20 queue-limit 2000 packets

  The **show policy-map interface** command shows correct rate but policing is failing.

  Conditions: The symptoms are observed on a Cisco Catalyst 6509, a WS-SUP32- GE- 3B, a Cisco 7600-SIP-400, a SPA-1XOC12-POS, a Cisco 7600-SSC-400 and a SPA- IPSEC-2G using a hierarchical policy with multiple parent shapers in user- defined classes and child policies with queuing and policing actions.

  Workaround: Remove "police cir percent" from child queuing policy "cbwfq- sip".

Alternate workaround: Use a different child-policy (with the same configuration). Example: Define a second policy-map, say “cbwfq-sip1”, with the same configuration as “cbwfq-sip” and change the cbwfq-ip as below: policy-map cbwfq-ip class tunnel13601 shape average 80000000 service-policy cbwfq-sip class tunnel13603 shape average 20000000 service-policy cbwfq-sip1 (shows a different child-policy with the same configuration as “cbwfq-sip”).

- CSCsl11712

  Symptoms: Router crashes when DGVPN is configured with VRF.

  Conditions: The symptom is observed with a Cisco 3845 router and when DGVPN is configured with VRF.

  Workaround: There is no workaround.

- CSCsl99156

  Symptoms:

  1. The No_Global bit (0x10) for MOI flag is incorrectly set for iBGP when it becomes best path.

  ```
  router#show ip cef vrf <vrf name> x.x.x.x int [snip] MPLS short path extensions: MOI
  flags = 0x16 <-------MOI flags 0x10 is incorrectly set for iBGP when it becomes best
  path, correct flag should be 0x4, 0x5, 0x6 ... correct now.
  ```

  2. The No_Global bit (0x10) for MOI flag for iBGP path was incorrectly unset when eBGP becomes best path.

     ```
     router#show ip cef vrf <vrf name> x.x.x.x int [snip] MPLS short path extensions:
     MOI flags = 0x5 <-------MOI flags 0x10 is incorrectly clear for ibgp path when
     eBGP becomes best path, correct flag should be 0x14, 0x15, 0x16... correct now.
     ```

  Conditions: This symptom sometimes happens after BGP path update.

  Workaround: Issue the **clear ip route vrf** *vrf name* **x.x.x.x/y command.**

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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*

- 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.

- CSCsu25016

  Symptoms: The **pppoe-client** command is not accepted on ATM interfaces. Cisco IOS software will report “% Unrecognized command” when an attempt is made to configure it.

  Conditions: This symptom is observed when an attempt is made to configure the **pppoe-client** command.

  Workaround: Use **pppoe_client** as the command prefix followed by the normal pppoe-client configuration items.

- 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.

- CSCsu47486

  Symptoms: Traceback seen while using the **mgcp block- newcalls** and **no mgcp block-newcalls** commands.

  Conditions: The symptom is observed only during repeated configuration/unconfiguration of **mgcp block-newcalls**.

  Workaround: There is no workaround.

- 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.

- CSCsu49132

  Symptoms: A router may crash when unconfiguring IPv6.

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

  Workaround: There is no workaround.

- CSCsu49204

Symptoms: A processor may crash while sending IMIX traffic at 80k packets per second (pps) across 30k PDPs. The system has 60k IP PDPs with Small Computer Systems Interface over IP (iSCSI) backup storage configuration.

Conditions: The following conditions trigger the crash (showing steps followed and sequence of events): - Create 60k IP PDPs. The charging gateway is down and there is no iSCSI back configuration. - Apply an iSCSI/GPRS-iSCSI configuration. - Send IMIX traffic at 80k pps across 30k PDPs. - After sending the traffic for about 10 minutes, the GPRS memory threshold is reached and some PDPs are deleted. - The processor will crash.

Workaround: There is no workaround.

- CSCsu49790

  Symptoms: PVC range disappears after a second PVC range is configured.

  Conditions: Occurs under the following scenario:

  1) Configure a PVC range on a point-to-point interface.

  2) Configure a second PVC range that approaches the maximum number of VCs possible.

  Workaround: There is no workaround.

- 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: 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.

- CSCsu54546

  Symptoms: When running an EasyVPN client on a router, the EasyVPN connection may go down and then renegotiate from the start whenever the ISAKMP lifetime expires.

  Conditions: The symptom is observed when running an EasyVPN client and whenever the ISAKMP lifetime expires.

Workaround: There is no workaround. You can increase the ISAKMP lifetime to 86400 to minimize service interruptions.

- 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.

- CSCsu58237

  Symptoms: A router may crash due to "TLB (load or instruction fetch) exception".

  Conditions: The symptom is observed when the **upgrade automatic** command is executed to download an image from cisco.com. This bug affects all IOS platforms that have the "Auto Upgrade Manager" feature.

  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".

- CSCsu61741

  Symptoms: The **lsp ping** command is missing.

  Conditions: This issue is specific to the Cisco 7301 router.

  Workaround: There is no workaround.

- 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 outage 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.

- CSCsu62175

  Symptoms: Error message with a traceback observed while configuring IPSec authentication/encryption for an IPv6 Open Shortest Path First (OSPF) process with no router-id.

  Conditions: The error message is issued when authentication or encryption is configured for an OSPFv3 process that has not been able to obtain a router-id.

  Workaround: Provide a loopback or other "up" interface with an IPv4 address, or use the **router-id** command to establish the OSPFv3 router-id before configuring OSPFv3 authentication or encryption.

- 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.

- CSCsu63996

  Symptoms: NSF restart may be terminated and OSPF NBR may flap during RP switchover. The **debug ip ospf adj** command shows the following message: OSPF: Bad request received.

  Conditions: The symptoms are observed when the links are broadcast networks and the restarting router is DR. It is seen when "nsf cisco" is configured and when some neighbors finish OOB resync much sooner than others.

  Workaround: Use the **nsf ietf** command.

  Alternate workaround: Configure routers so that the restarting router is not DR (use OSPF network type point-to-point or priority 0).

- 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 Cisco 7201 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 is enabled LDP/IGP synchronization using 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 - 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.

- 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.

- CSCsu69687

  Symptoms: A slow start call may fail.

  Conditions: The symptom is observed with an H323 slow start call.

  Workaround: Use fast start or tunneled calls instead of slow start.

- 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.

- CSCsu72700

  Symptoms: HWIC-AP-EU is not detecting Staggered PRF radars which operate in the 5600-5650 band of channels.

  Conditions: The symptom is observed when the router has a European HWIC-AP and is running in 5 GHz mode.

  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.

- CSCsu73867

  Symptoms: After configuring address-family IPv6 & VPNv6, there is no option for the **maximum-paths** <*range*> command.

  Conditions: Occurs in a Cisco 7200 running Cisco IOS Release 12.4(22)T.

  Workaround: There is no workaround.

- CSCsu74400

  Symptoms: A device running FTP to transmit the DHCP database may experience a file descriptor leak that results in errors such as:

  ```
  ROUTER#show run
  ```
  OR
  ```
  ROUTER#show start Using XXXX out of XXXX bytes %Error opening nvram:/startup-config
  (Bad file number)
  ```
  OR
  ```
  ROUTER#dir nvram: Directory of nvram:/ %Error opening nvram:/ (File table overflow)
  XXXX bytes total (XXXX bytes free)
  ```
  Conditions: Occurs when the router is configured to use FTP to transmit the DHCP database:

  ip dhcp database ftp://XXXX:XXXX@X.X.X.X/XXXX

  And the FTP server becomes unreachable. The file descriptor leak can be viewed in the output of **show file descriptors**:

  ```
  ROUTER-B#show file descriptors File Descriptors:
  FD Position Open PID Path 0 0 0302 145 ftp://X.X.X.X/DHCP 1 0 0302 145
  ftp://X.X.X.X/DHCP 2 0 0302 145 ftp://X.X.X.X/DHCP 3 0 0302 145 ftp://X.X.X.X/DHCP 4 0
  0302 145 ftp://X.X.X.X/DHCP 5 0 0302 145 ftp://X.X.X.X/DHCP 6 0 0302 145
  ftp://X.X.X.X/DHCP 7 0 0302 145 ftp://X.X.X.X/DHCP 8 0 0302 145 ftp://X.X.X.X/DHCP 9 0
  0302 145 ftp://X.X.X.X/DHCP <snip>
  ```
  Workaround: Ensure that the FTP server does not become unreachable for more than 128 total minutes, as there are only 128 file descriptors. In the event that all 128 file descriptors are leaked, a reboot is required to recover.

- 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 IOS code that supports SSLVPN. Once the router is reloaded SSLVPN takes over the ACL time-ranges and these time ranges are no longer work for ACLs.

Workaround: Reconfigure the configuration mode ACL time-ranges after the reboot.

Further Problem Description:

show startup-configuration 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.

show running-configuration 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.
```

- 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 command **sh oer border active-probes** 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.

- CSCsu78451

  Symptoms: The command **webvpn create template** shows “svc- translation-table” as one of the options when giving a “?” on the CLI, when this option should be hidden.

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

  Workaround: There is no workaround.

  Further Problem Description: The “svc-translation-table” option is not supported at this time. Therefore it should be hidden. There are, however, no side effects to this issue.

- 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.

- CSCsu82166

  Symptoms: The **copy** command may drop forward slashes in directory paths. This breaks all copying to and from the router.

  Conditions: This occurs in a router running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCsu87180

  Symptoms: The MPLS support command is missing.

  Conditions: The symptom is observed with a Cisco 3270 router that is running Cisco IOS Release 12.4(15)T or Release 12.4(20)T.

  Workaround: There is no workaround.

- 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.

- CSCsu90280

  Symptoms: IPv6 DMVPN tunnel does not work. IPv6 NHRP registration between Hub and Spoke fails.

  Conditions: The symptoms are observed under normal operation.

  Workaround: There is no workaround.

- CSCsu92395

  Symptoms: Router crashes.

  Conditions: This issue occurred on a Cisco 870 router running Cisco IOS Release 12.4(15)T7 and 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.

- CSCsu93374

  Symptoms: The group state of a slave group may unexpectedly change to Active after an RP switchover.

  Conditions: The symptom is observed when HSRP multigroup is configured such that a slave group follows the state of a master group. If the HSRP group state is Standby, then the group state of the slave group may change to Active after an RP switchover.

  Workaround: There is no workaround.

- CSCsu97507

Symptoms: After removing one of “ip name-server xxxx” entries, the command **show ip dns view** displays broken output.

Conditions: The symptoms are observed with the following steps:

3. Add several “ip name-server xxxx”.
4. Remove one of the middle entries.
5. 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”, it shows “na^@^@”; enter “show version”, 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.

- CSCsv00928

  Symptoms: If HTSP is null, using it to reference other data members will cause a traceback or crash on router.

  Conditions: This occurs when the condition enters into off hook state and HTSP is null.

  Workaround: There is no workaround.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24.

- 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.

- 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.

- 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.

- 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.

- CSCsg39977

  Symptom: 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.

- 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.

- 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.

- 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.

- 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".

- CSCsj56281

  Symptoms: Inherit peer-policy does not work after router reload.

  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.

- CSCsk87526

  Symptoms: The following traceback is seen:

  ```
  %IPV6-3-INTERNAL: Internal error, Protocol <protocol>, decrement of zero ref count
  ```

Conditions: The traceback may be seen when the following conditions are met:

- Two or more instances of the same IPv6 routing protocol are configured. For example, two instances of OSPFv3 are configured.
- A particular route is first learned by one instance of the protocol, then by the second instance at a better metric.
- The IPv6 routing table is cleared with the **clear ipv6 route *";** command or the first instance of the routing protocol is shut down.

Workaround: There is no workaround.

- CSCsk98751

  Symptoms: A router may crash after the command **mpls traffic-eng backup-path tunnel** 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.

- 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 **clear mpls tra auto-tunnel primary** followed by **clear mpls tra auto-tunnel backup** command. This crash could happen with or without a SSO switchover before issuing those commands.

- 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.

- 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.

- CSCsm82264

  Symptoms: When standby boots up, deadlock could happen, causing the standby to crash. Also can happen when the call-home process is restarted on active, causing the active supervisor to crash.

  Conditions: This problem depends on timing. Occurs after configuration changes could alter bootup timing.

  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.

- CSCso19662

  Symptoms: Tracebacks are seen after unconfiguration when using the **clear ip nat translation *** command.

  Conditions: Cisco device with NAT configure. Not platform dependant

  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.

- 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”.

- 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.

- 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.

- 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.

- CSCsq06208

  Symptoms: When health monitoring (HM) diagnostic failure happens, call-home diagnostic messages are not out before platform action is taken.

  Conditions: Call-home is subscribed to diagnostic alert group minor or major error and the gold policy is active. It only happens when the HM diagnostic test interval is small enough.

  Workaround: Set the HM diagnostic test interval to be large enough, but there is no guarantee it will work in all test cases.

  Further Problem Description: Because gold policy is last policy in EEM queue, it waits for call-home messages to send out before it executes. If gold policy continues to trigger on the next test failure after reaching the threshold when action notify flag is already false, it does not need to wait for call-home message to execute. It could crash the system before the call-home message for the last gold policy finishes.

  Adding ACTION_NOTIFY TRUE condition to the gold policy will prevent the gold policy to continuously execute and consistent with call-home message triggering condition.

- 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**.

- 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.

- CSCsq39254

  Symptoms: When call-home profiles are removed by the **no profile all** command, the standby system will reload if a new profile is added or a Cisco TAC profile is edited.

  Conditions: The symptom is observed when a non-default call-home profile is configured, and then removed by the **no profile all** command. The problem will occur when customer tries to add new profile or to edit a Cisco TAC profile.

  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.

- 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.

- 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.

- 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.

- CSCsq75661

  Symptoms: An ATM interface that is configured with a large number of PVCs may exhibit PVC provisioning problems after repeated interface flaps. The VCC count on the ATM interface would increase by a random number once after each flap.

  Conditions: This symptom is observed on a dual PRE2 system that is running Cisco IOS Release 12.2(31)SB12 code and operating in SSO mode.

  Workaround: Router reload or PRE cutover.

- 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.

- 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.

- 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.

- 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).

- 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.
  ```

- 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.

- CSCsr09370

  Symptoms: Multiple responses are received when a multicast group is pinged from the source in an MVPN environment.

  Conditions: This symptom is observed with a Cisco 7200 router that is running Cisco IOS Release 12.4(21.5)PI9A.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080708-dns

- 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”.

- 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.

- CSCsr40997

  Symptoms: When a router interface is shut, the prefix attached to the interface is not advertised with infinite metric out the other interfaces.

  Conditions: Occurs when route is configured for RIP for IPv6 (RIPng)

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCsr56311

  Symptoms: When fragmented skinny packets transverse the router, the router may unexpectedly reload due to bus error.

  Conditions: Can occur on routers running NAT.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsr61532

  Symptoms: Router may experience dropped packets.

  Conditions: Occurs when passive probing is configured with mode select-exit best. A prefix is rotated through all exits for holddown time to get passive performance on all exits. In doing so, if a link is already overloaded, putting prefix on the overloaded link can cause the performance to further deteriorate.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsu24474

  Symptoms: MPLS TE tunnel may not come up due to signalling failure. The RESV message from the TE tail end is being dropped at a node which is configured with an identical APS protect IP address as the downstream node (which uses same IP address but is APS active).

  Conditions: The symptoms are observed with an interface in the “admin up, line down” state that has an identical IP address same as that of a downstream node. An MPLS TE tunnel having record route enabled needs to pass through both the nodes. This will cause RESV to be dropped at the node having the “admin up, line down” interface with the same IP address.

  Workaround: Disable Record-route.

- CSCsu62356

  Symptoms: Under certain conditions the RIP for IPv6 (RIPng) “Last Gasp” message (all metrics infinite) does not get sent.

  Conditions: This is seen under high load or on routers with large numbers of interfaces.

  Workaround: There is no workaround but routes will eventually time out.

- 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.

- CSCsv12265

  Symptoms: An HSRP group with a valid configuration remains in the INIT state of an active interface.

  Conditions: The symptom occurs when the HSRP group is configured to use a learnt IP address, using the **standby <group> ip** command, and the interface IP address has recently been changed without involving a shutdown of the interface.

Workaround: If you wish to change the interface IP address, then the interface should be shutdown while the address is changed and made active after the new address is in place.

- 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.

- 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.

- 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.

- 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.

- CSCsr85757

  Symptoms: IGMPv3 not enabled on VLAN as expected

  Conditions: By default **ip igmp snooping** enables IGMP snooping on a VLAN, but in the failed case it is not enabled.

  Workaround: There is no workaround.

- 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:
  A000000001000026000000F5 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.

- 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.

- 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.

- 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.

- 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.

- CSCsu24505

  Symptoms: Router may crash and reload intermittently with TLB (load or instruction fetch) exception.

  Conditions: Occurs when a device is configured to support NTP, and is running one of the following Cisco IOS Releases:

  12.4(15)XZ

  12.4(15)XZ1

  12.4(20)T

  12.4(20)T1

  12.4(20)YA

  12.4(20)YA1

  12.4(22)MD

  12.4(22)T

  Workaround: Temporarily remove the NTP servers from the configuration with these commands:

  no ntp server x.y.z.w no ntp peer a.b.c.d

- 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.

- 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.

- CSCsu40077

  Symptoms: When doing MAC authentication bypass and dot1x and having “dot1x tx-period” timers aggressive (like 3), you can end up with the port being in UNAUTHORIZED state according to the switch although traffic is flowing just fine.

  Conditions: This was seen on a Cisco 2960 running Cisco IOS Release 12.2(46)SE and mab+dot1x+timer of 3 configured.

  Workaround: Increase tx-period timer.

- 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.

- 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.

- CSCsu49922

  Symptoms: When attempting to connect to a Cisco 181x or Cisco 186x router using the client-less SSLVPN feature, users may experience connection issues caused by session hangs.

  Conditions: This is seen only when using SSLv3, client-less mode, and the hardware crypto engine.

  Workaround: Choose one of the following alternatives: * Use TLSv1.x as the SSL protocol * Disable the hardware crypto engine using the **no crypto engine accelerator** command * Use thin client or AnyConnect client.

- 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.

- CSCsu56748

  Symptoms: Spurious memory seen in unit test while pinging from generator to reflector.

  Conditions: Occurs while the ping passes through router after applying the crypto map. If the crypto map is not configured then the spurious memory not be seen.

  Workaround: There is no workaround.

- CSCsu64166

  Symptoms: Cisco Express Forwarding (CEF) packet is dropped on tunnel interface when IPSec tunnel is unconfigured and a tunnel is configured on a loopback interface.

  Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(21.14)T2.

  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.

- CSCsu64933

  Symptoms: When using CTCP between an EzVPN server and remote client, with one-way traffic, the receiver does not send gratuitous ACKs for the received packets.

  Conditions: If there is a firewall between client and server, it will drop all subsequent packets once the maximum TCP window size is exceeded.

  Workaround: If the traffic is being sent at a slower rate, use periodic DPDs to help reset the window size to prevent the sender from going over the maximum window size. Or disable TCP sequence number checks on the firewall in between.

- 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.

- 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 1 interface Ethernet1/0 line-protocol interface Ethernet 0/0 standby 1 track 1

  Workaround: Use **show tracking** instead, or configure tracking with the new command.

- 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.

- 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.

- CSCsu79988

  Symptoms: Before this BGP aspath memory optimization, the memory consumption for aspath has increased. With this memory optimization, the memory consumption for aspath has reduced.

  Workaround: There is no workaround.

- CSCsu88107

  *Packets generated by router from IVRF to FVRF don't hit the crypto map

- 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.

- 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.

- 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.

- CSCsv03300

  Symptoms: Cisco 7200 NPEG2 router crashes while displaying the interface output for onboard gigabit ethernet using the **show interface gig0/x** command.

  Conditions: Occurs when a CBWFQ QoS policy is attached to the onboard gigabitethernet interface.

  Workaround: There is no workaround.

- 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.

- CSCsv04325

  Symptoms: When the EzVPN session is up, the **show crypto session** output will show corrupted value for internet key exchange (IKE) lifetime.

  Conditions: Occurs randomly. Unknown conditions.

  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.

- 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.

- CSCsv12510

  Symptoms: Service policy is removed from the map-class when configuring a "mincir" equal to the full interface committed information rate (CIR).

  Conditions: This issue is seen on a Cisco 7200 router.

  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.

- 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.

- 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.

- 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: ASR Router goes down.

  Conditions: Occurs when kron policy is configured and SCP is used.

  Workaround: Use regular SCP.

- 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.

- 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.

- 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.

- 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.

- CSCsv36892

  Symptoms: TCLsh mode is not exited when the session is disconnected or times out. The next user to connect and authenticate is put in TCLsh mode.

  Conditions: Occurs on high availability systems with an active and standby RP.

  Workaround: Explicitly exit TCLsh mode rather than disconnecting or allowing the session to time out.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp.

- CSCsv38205

  Symptoms: Running a post-dial delay operation with reaction configuration may cause a router to crash after removing the operation.

  Conditions: The symptom is observed when using a post-dial delay operation with reaction configuration.

  Workaround: Do not use reaction configuration for post-dial delay.

- CSCsv38804

  Symptoms: VIC2 BRI Layer 2 will not come up after boot up.

  Conditions: The symptom is observed with VIC2-2BRI-NT/TE cards.

  Workaround: There is no workaround.

- CSCsv40012

  Symptoms: Router crashes when the **no frame-relay interface-dlci 300** command is issued from the VTY.

  Conditions: This symptom is observed on a Cisco router that is configured with the **frame-relay interface-dlci 300** on the console. If the **no** form of the command is entered from the VTY, the crash occurs. In this mode when giving the command “load-interval 30" in the console, router crashes.

  Workaround. There is no workaround.

- 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.

- 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 NAT 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 NAT 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.

- CSCsv42275

  Symptoms: Unable to delete VPN routing/forwarding (VRF) created using a VRF definition.

  Conditions: Occurs in Cisco IOS Release 12.4T. The **no vrf definition** command does not delete the VRFs.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCsv54324

  Symptoms: Hot Standby Routing Protocol (HSRP) router stuck in INIT state.

  Conditions: Problem is seen after a reload

  Workaround: Use the **clear interface** *interface-type interface-number* command or perform a **shut/no shut** on the interface.

- CSCsv54510

  Symptoms: The router is not getting pruned after shutting the interface. The pruned flag is not getting set even after waiting for long time.

  Conditions: Happens with a Cisco 7200 router running Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCsv62133

  Symptoms: Call transfer failing on Call Manager while connected through a SIP trunk.

  Conditions: SIP trunk using UDP with packet losses in network.

  Workaround: There is no workaround.

- CSCsv62225

  Symptoms: Router crashed when PPPoE sessions were cleared and policy was removed.

  Conditions: This symptom occurs while removing policy using **no policy-map name**

  Workaround: There is no workaround.

- CSCsv62777

  Symptom: 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: The symptom is observed when an extended ping with CLNS is done and not completed.

  Workaround: Reload the router.

- 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.

- CSCsv68398

  Symptoms: The RPM-PR Card does not boot up, because it does not receive the boot acknowledgment from the PXM and reboots continuously.

  Conditions: Seen during normal bootup of RPM-PR card.

  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.

- 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

  Symptoms: Sending control packets to read the associations and peer, system variable crashes the router.

  Conditions: The crash occurs only on generation of control packets to the router.

  Workaround: Do not generate control packets to router.

- CSCsv76862

  Symptoms: A Cisco router running a version of code that contains the Embedded Event Manager (EEM) version 3.0 or EEM version 3.1 may:

  * Allow a policy in the user policy directory to be registered as a system run-type policy. * Allow a policy to be registered where the user specifies a type of system but the policy is registered as a run-type user policy. * Require the user to specify a type of user when registering a policy to override a system policy. * Prevent a policy that was registered with a type of user specified in the policy registration command to be unregistered using the no form of the policy registration command. * Not generate a configuration command when a default option to Mandatory policy is changed so the change can not be saved to the startup-config. * Not generate a configuration command when a user policy is being used to override a system Mandatory policy so the user policy will need to be re-registered after every bootup. * Leak memory when a Mandatory policy is registered and unregistered and an error occurs.

Conditions: These occur in Cisco IOS and Cisco IOS software modularity versions that contain EEM version 3.0 and EEM version 3.1. EEM versions 2.4 and earlier are not affected. Users can check what version of EEM is in their image by using the **show event manager version** command that was introduced in EEM version 2.4.

Workaround: There is no workaround.

Further Problem Description: The EEM command to register a policy is:

event manager policy *filename.tcl*

This command has an option to specify a type of either *system* or a type of *user*. This option is designed to allow the user to specify which directory is searched when looking for the policy to register. If the user specifies a type of system, the system policy directory (hardcoded in the image) is searched for a policy with the filename specified. If the user specifies a type of user, only the user policy directory (which must be configured with the **event manager directory user policy** *device:directory* command) is searched. If the user does not specify a type, first the user policy directory is searched and if no policy is found then the system policy directory is searched - this allows the user to override a system policy with a user policy and not have to specify a type of user.

The concept of which directories are searched when registering a policy is different from the concept of which run-type the policy is registered with. The run-type specifies the privilege level that the policy will execute with. System policies have full privileges. User policies are limited to the privileges of Safe-Tcl with a few exceptions that are covered in the EEM documentation. The run-type of the policy is determined by the following rules:

* If a policy is in the system policy directory at the time it is being registered, that policy will be registered with a run-type of system.

* If a policy is in the user policy directory at the time it is being registered and it does not contain a valid Cisco digital signature it will be registered with a run-type of user. Exception: If the policy is in the user policy directory at the time it is being registered and it contains a valid Cisco digital signature it will be promoted to a run-type of system.

The problems described in this bug occur because of an implementation that jumbled these two concepts together.

- 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.

- CSCsv91838

  Symptoms: A router may crash and the following traceback may be seen:

  Traceback= 0x6141BE68 0x6141CF74 0x6141E3F0 0x619D2A04 0x619D3150 0x619F8950 0x633C68D8 0x633C68BC

  Conditions: The symptoms are observed on a Cisco 3825/3725 with WIC/HWIC ADSL/SHDSL cards and when the **atm video aesa default** command is executed on the ATM interface. It is seen with the c3825-adventerprisek9-mz.124-21.14.T1 and c3825-adventerprisek9-mz.124-23.7.T images.

  Workaround: There is no workaround.

- 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.

- CSCsv93351

  Symptoms: The CNS id (config, event and/or image) changes unexpectedly.

  Conditions: The command **cns id with argument** *ipaddress* is configured. Then whenever any interface changes its IP address, the CNS ID will change to be the IP address of the interface that just had a change of IP address.

  For example, the following 3 commands may cause this problem:- **cns id FastEthernet 0/0 ipaddress**, **cns id FastEthernet 0/0 ipaddress event** or **cns id FastEthernet 0/0 ipaddress image**

  Workaround: Use the command **cns id** with argument *string* instead.

- CSCsv95977

  Symptoms: DCN sent during Phase B when testing Cisco 5510 to Cisco 5510 SG3 spoofing.

  Conditions: This defect only affects DSP firmware versions 24.2(00)DSP.

  Workaround: There is no workaround.

- CSCsv99335

  Symptoms: If HTSP is NULL, using it to reference other data members will cause a traceback or may cause the router to crash.

  Conditions: The symptom occurs when the condition enters into an offhook state and HTSP is NULL. It is very rare for HTSP to be NULL and is only detected by SA.

Workaround: There is no workaround.

- CSCsv99662

  Symptoms: Traffic of newly created VLAN not running between two ports on different HWIC when these two HWICs are stacked.

  Conditions: Occurs when two HWICs (HWIC-4ESW and HWIC-D-9ESW) are stacked in a Cisco 2811 router.

  Workaround: There is no workaround.

- CSCsw15188

  Symptoms: Router crashes when enabling **debug isdn q931**

  Conditions: Problem happens when logging debugs from **debug isdn q931** to an external syslog server.

  Workaround: Disable the syslog server when doing the debugs.

- CSCsw16658

  Symptoms: "A named IPv6 access list with this name already exists" error incorrectly occurs in following scenario and we can not create ipv4 access-list:

  1. Configure **snmp-server community public RW ipv6** <*access-list name*> (Example. sample).

  2. Unconfigure it using **no snmp-server community public RW ipv6** <*access-list name*> (Example. sample).

  3. Try to create access-list name, same as ipv6 access-list name which was given in step 1.

  After step 2, we are not seeing IPv6 access-list neither in running-config nor **show ipv6 access-list**, but still we are not able to configure ipv4 access-list.

  Conditions: Problem seen with the router loaded with c7200-adventerprisek9-mz.124-23.8.T image.

  Workaround: There is no workaround.

- 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.

- 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 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.

- CSCsw30602

  Symptoms: Getting tracebacks and spurious memory when round-robin is configured under “cfg-dns-view”.

  Conditions: This can be seen in router loaded with c7200-adventerprisek9-mz.124-23.8.T image.

  Workaround: There is no workaround.

- CSCsw30921

  Symptoms: Getting tracebacks and spurious memory access when unconfiguring “appfw” policy with empty name attached to “IP inspect name <WORD>”.

  Conditions: This can be seen in router loaded with c7200-adventerprisek9-mz.124-23.8.T.

  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.

- CSCsw31504

  Symptoms: The “fqdn” string within PKI trustpoint becomes corrupted.

  Conditions: Corruption occurs during CA rollover.

  Workaround: Do not manually configure the “fqdn” for the device and instead rely on the contents of the hostname+domain-name within the global configuration.

- CSCsw34224

  Symptoms: A router may reload unexpectedly.

  Conditions: The symptom is observed when configuring “auto qos/discovery” on the ATM SVC.

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.

- 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.

- CSCsw39851

  Symptoms: Router crashes with "nemov6_show_bce".

  Conditions: This occurs on Cisco 7200 routers running Cisco IOS Release 12.4(24)T when mobile router with IPv6 has been configured.

  Workaround: There is no workaround.

- CSCsw39985

  Symptoms: Too many IPC error messages are seen.

  Conditions: The symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.4 with dLFIoLL configuration. The standby router cannot be accessed when the router is HA setup.

  Workaround: There is no workaround.

- CSCsw40248

  Symptoms: Service policy disappears after removing and attaching to other class-maps under the same policy-map.

  Conditions: The symptom is observed with a router that is running Cisco IOS Release 12.4(23.10)T.

  Workaround: There is no workaround.

- CSCsw41706

  Symptoms: A Cisco router may unexpectedly reload or produce an error similar to the following:

  Embedded Event Manager configuration: failed to stage user library directory <device>:<directory>: error creating file

  Conditions: This occurs when trying to configure the **event manager directory user library** *device:directory* command.

Workaround: There is no workaround.

- CSCsw42564

  Symptoms: Router reloads at "qos_preclassify_cmd".

  Conditions: Occurs while configuring **qos pre-classify** under "crypto dynamic-map" after unconfiguring it using VTY.

  Workaround: There is no workaround.

- 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 command **bridge-group 1** is removed from the sub-interface, it will behave as expected.

- 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".

- 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

  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

- 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.

- 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 Cisco IOS Release prior to 12.4(15)T7.

- CSCsw65059

  Symptoms: Router crashed after executing the command **authentication username """" password "qwqwqwrw** and checking in running-configuration.

  Conditions: Occurs on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsw65303

  Symptoms: Spurious access occurs when pattern is configured with repeating numbers.

  Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(23.11)T.

  Workaround: Use a pattern without repeating numbers.

- CSCsw67040

  Symptom: A Cisco 5850 may crash.

  Conditions: The symptom is observed on a Cisco 5850 that is running Cisco IOS Release 12.4(23).

  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.

- 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.

- 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.

  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”.

  Condition: 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.

- CSCsw75589

  Symptoms: If you have configured Netflow and also have “ip flow-cache mpls label-positions”, you are very likely to run in a bus error crash with info similar to what is seen here:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 10:28:28 UTC Sat Dec 20 2008
  addr=0x1E, pc=0x61CB7180, ra=0x61CBA5C0, sp=0x65BCAF20
  %ALIGN-1-FATAL: Illegal access to a low address 10:28:28 UTC Sat Dec 20 2008
  addr=0x1E, pc=0x61CB7180, ra=0x61CBA5C0, sp=0x65BCAF20
  10:28:28 UTC Sat Dec 20 2008: TLB (store) exception, CPU signal 10, PC = 0x61CB7180
  ```

  Conditions: Problem is platform independent but specific to Cisco IOS release. This problem is seen in Cisco IOS Release 12.2(33)SRC1 and possibly affects Cisco IOS Release 12.4T releases as well.

  Workaround: Consider removing MPLS netflow configuration by removing the **ip flow-cache mpls label-postion 1** command.

- 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.

- CSCsw77247

  Symptoms: Unconfiguring frame-relay map with NULL vc-bundle name results in trace-back.

  Conditions: This happens on a Cisco router running Cisco IOS Release 12.4(23.12)T.

  Workaround: There is no workaround.

- CSCsw78806

  Symptoms: Router crashes while configuring “lat host” with empty string under dialer interface.

  Conditions: It is happening on a router running the c7200-adventerprisek9-mz.122-32_8_11_SR171 image.

  Workaround: There is no workaround.

- CSCsw80206

  Symptoms: Build failure for the Cisco 880 series.

  Conditions: This is a side effect of the CSCsw72677.

  Workaround: There is no workaround.

- CSCsw85235

  Symptoms: FTP copy fails, giving the error message “Incorrect Login/Password”.

  Conditions: The symptom is observed when copying a file using FTP and using the username and password in the command itself.

  Workaround: Set FTP username/password in router using the **ip ftp** command.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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/en/US/products/csa/cisco-sa-20100324-sccp.html.

- CSCsy73268

  Symptoms: When ISDN PRI is configured in trunkgroups, and when MCID scrip is initiated, the call fails as the script cannot identify that the call leg is part of a trunkgroup ISDN.

Conditions: This symptom is seen only when ISDN trunkgroups are configured when running MCID script.

Workaround: Without ISDN trunkgroups configured, the MCID script works as expected.

Resolved Caveats—Cisco IOS Release 12.4(22)T5

Cisco IOS Release 12.4(22)T5 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)T5 but may be open in previous Cisco IOS releases.

- CSCee93607

  Symptoms: A VPN client cannot connect to a router that functions as an EzVPN server.

  Conditions: This symptom is observed on a Cisco router that functions as an EzVPN server when the user name is not sent in the RADIUS authentication request for the VPN client, causing the authentication server to reject the VPN client.

  Workaround: If this is an option, use local authentication.

  Further Problem Description: The following error message appears in the debug output:

  ISAKMP (0:1): FSM action returned error: 4

- CSCsx26025

  Symptoms: Wireless clients are not able to ping each other after a few minutes.

  Conditions: Can occur on any of the following routers with 802.11 wireless interfaces:

  UC500, 85x, 87x, 1811, HWIC-AP

  Workaround: There is none.

- CSCsy30256

  Symptoms: A Cisco 2811 router crashes due to a bus error after an ISDN call terminates. The following is seen before the crash:

  ```
  %ALIGN-1-FATAL: Corrupted program counter
  pc=0x0 , ra=0x400ABA78 , sp=0x44647440
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x0
  ```

  Conditions: The symptom is observed when “dialer rotary-group *number*” is configured on the interface.

  Workaround: Use “dialer pool” instead of “dialer rotary”.

- CSCsy61321

  Symptoms: Accounting requests sent to the TAC server do not fail over to the second server.

  Conditions: This symptom is observed when two TACACS servers are configured, the first without TACACS, the second with TACACS, and authentication is configured as "none"

  Workaround: Use a single working server, or ensure that the first group uses a valid server.

- CSCsy74023

  Symptoms: A slow memory leak occurs, mainly in the 72 bytes, 80 bytes, and possibly 192 bytes memory regions blocks.

  Conditions: This symptom is observed with a large number of IPSec peers (greater than 100) and several thousand tunnels when Phase I is authenticated by RSA-SIG.

  Workaround: There is no workaround.

- CSCta09049

  Symptoms: A memory leak chunk in alloc-proc "encrypt proc" with the name "Packet Header" is observed.

  Condition: This symptom is observed with software crypto enabled. The same configuration and traffic running with onboard-VPN does not have the leak.

  Workaround: Configure "no ip cef optimize neighbor resolution".

- CSCta32825

  Symptoms: A Cisco router may crash with a bus error after configuring a class-map or modifying a class-map.

  Conditions: This symptom is observed when using the **class-map** command in global configuration mode and the **match** command in class-map configuration mode. For example, entering the following commands may result in a crash:

  ```
  *router(config)#class-map match-any PRIO
  *router(config-cmap)#match dscp cs4
  *router(config-cmap)#match dscp cs4 af41
  *router(config-cmap)#match dscp cs4 af41 af42
  *router(config-cmap)#match dscp cs4 af41 af42 af43
  *router(config-cmap)#match dscp cs4 af41 af42 af43 ef
  *router(config-cmap)#match dscp cs4 af41 af42 af43 ef cs5 <---device crashes here
  ```

  Workaround: Configure QoS changes when no traffic is passing through the router. This has only been seen while traffic is trying to match against the policy while it is being updated.

- 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.

- CSCta69213

  Symptoms: A Cisco router configured for NHRP may crash due to a bus error.

  Conditions: This symptom is observed on a Cisco router configured for NHRP and DMVPN.

  Workaround: There is no workaround.

- CSCta86675

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

  Conditions: This symptom occurs when stress traffic passes through a Cisco router that is configured with QOS policies, cryptomap, and access-lists.

  Workaround: There is no workaround.

- CSCtb33439

  Symptoms: Hub or spoke crashes when the spoke tunnel is shut or unshut.

  Conditions: This symptom occurs when applying DMVPN configurations and doing a **shutdown** and **no shutdown** of the tunnel.

  Workaround: There is no workaround.

- CSCtc51539

  Symptoms: A Cisco router crashes with a "Watch Dog Timeout NMI" error message.

Conditions: This symptom is observed only on devices configured with Bidirectional Forwarding Detection (BFD). For further information on BFD, consult the following link:

http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

Workaround: Disable BFD.

- 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.

- 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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-igmp.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://tools.cisco.com/security/center/content/CiscoSecurityBundle/cisco-sa-20100922-bundle

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- 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 the **clear pppoe all** command is entered:

```
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 the **line-mode 4-wire enhanced** command.

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.

- 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.

- 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.

- 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.

- CSCtf42216

  Symptoms: The **no shutdown** command will not take effect if done immediately after executing the **shutdown** command under voice-port.

  Conditions: This symptom occurs when executing a **no shutdown** command after the **shutdown** command. The **no shutdown** command will not get executed immediately and will be ignored. User has to re-enter the **no shutdown** command a few seconds later.

  Workaround: Wait a few seconds to re-enter the **no shutdown** command.