Caveats for Cisco IOS Release 15.1(3)T

Caveats

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

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

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

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

This document contains the following sections:

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

Resolved Caveats—Cisco IOS Release 15.1(3)T4

Cisco IOS Release 15.1(3)T4 is a rebuild release for Cisco IOS Release 15.1(3)T. The caveats in this section are resolved in Cisco IOS Release 15.1(3)T3 but may be open in previous Cisco IOS releases.

- CSCsv30540

  Symptoms: The error message %SYS-2-CHUNKBOUNDSIB and a traceback are seen.

  Conditions: This symptom is observed when the **show running-config/write memory** command is issued.

  Workaround: There is no workaround.

- CSCtj48387

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

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

  Workaround: There is no workaround.

- CSCtn65116

  Symptoms: Some VPNv4 prefixes may fail to be imported into another VRF instance after a router reload or during normal operation.

  Conditions: This symptom is observed with a router that is running BGP and Cisco IOS Release 12.2(33)SB or Cisco IOS Release 12.2(33)SRB or later releases. Earlier versions are not affected. This occurs with the same prefixes with different mask lengths, for example, 10.0.0.0/24 and 10.0.0.0/26 (but not for 10.0.0.0/24 and 10.0.0.1/32, because 10.0.0.0 is not the same prefix as 10.0.0.1). This issue is seen with the following process:

  1. Assume the prefix, 10.0.0.0/24, is imported from VPNv4 to VRF. It has been allocated a label of 16.
  2. The allocated label changes from 16 to 17, for example, due to interface flapping or BGP attribute change.
  3. However, before the BGP import happens, a more specific prefix (for example, 10.0.0.0/26) is added to the BGP radix tree, but it is denied for importing due to, say, the RT policy.

  Workaround: Remove the RT or import map and add it back. Note, however, that if the above conditions occur again, the issue could reappear.

- CSCtq24557

  Symptoms: The router crashes after deleting multiple VRFs. This happens very rarely.

  Conditions: This symptom is observed in a large scale scenario.

  Workaround: There is no workaround.

- CSCtq59923

  Symptoms: OSPF routes in RIB point to an interface that is down/down.

  Conditions: This symptom occurs when running multiple OSPF processes with filtered mutual redistribution between the processes. Pulling the cable on one OSPF process clears the OSPF database, but the OSPF routes associated with the OSPF process from that interface still point to the down/down interface.

  Workaround: Configure “ip routing protocol purge interface”.

- CSCtq78217

  Symptoms: A router crashes with the following information:

  ```
  System returned to ROM by address error at PC 0xZZZZZZZZ, address 0xZZZZZZZZ
  ```

  Conditions: This symptom is observed with CUBE + SIP.

  Workaround: There is no workaround.

- CSCtr86328

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

  Conditions: This symptom is observed when a Cisco IOS device is configured for clientless SSL VPN.

  Workaround: There is no workaround.

  Further Problem Description: This problem has been seen when the stock Andorid 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

- CSCtr88739

  Symptom 1: Routes may not get imported from the VPNv4 table to the VRF. Label mismatch may also be seen.

  Symptom 2: The routes in BGP may not get installed to RIB.

  Conditions: These symptoms are only observed with routes with the same prefix, but a different mask length. For example, X.X.X.X/32, X.X.X.X/31, X.X.X.X/30 ..... X.X.X.X/24, etc. These issues are not easily seen and are found through code walkthrough.

  For symptom 1, each update group is allocated an advertised-bit that is stored at BGP net. This issue is seen when the number of update groups increases and if BGP needs to reallocate advertised-bits. Also, this symptom is observed only with a corner case/timing issue.

  For symptom 2, if among the same routes with a different prefix length, if more specific routes (15.0.0.0/32) do not have any bestpath (for example, due to NH not being reachable or inbound policy denying the path, but path exists due to soft-reconfiguration), then even if a less specific route (15.0.0.0/24) has a valid bestpath, it may not get installed.

  Workaround for symptom 1: Remove "import-route target" and reconfigure route-target.

  Workaround for symptom 2: Clear ip route x.x.x.x to resolve the issue.

- CSCts70790

  Symptoms: A Cisco 7600 router ceases to advertise a default route configured via "neighbor default-originate" to a VRF neighbor when the eBGP link between a Cisco 7600 router and its VRF eBGP peer flaps.

Conditions: This symptom is observed when another VPNv4 peer (PE router) is advertising a default route to the Cisco 7600 router with the same RD but a different RT as the VRF in question. When the VRF eBGP connection flaps, the VRF default is no longer advertised.

Workaround: Remove and readd the **neighbor default-originate** command on the Cisco 7600 router and do a soft clear for the VRF neighbor.

- CSCtt02313

  Symptoms: When a border router (BR) having a parent route in EIGRP is selected, “Exit Mismatch” is seen. After the RIB-MISMATCH code is integrated, RIB-MISMATCH should be seen, and the TC should be controlled by RIB-PBR, but they are not.

  Conditions: This symptom is observed when two BRs have a parent route in BGP and one BR has a parent route in EIGRP. The preferable BR is the BR which has a parent route in EIGRP. The BRs having BGP have no EIGRP configured.

  Workaround: There is no workaround.

- CSCtt26721

  Symptoms: A Cisco router may see increased CPU utilization when NBAR is used.

  Conditions: This has been experienced on a Cisco 3925 router running Cisco IOS Release 15.1(3)T2.

  Workaround: There is no workaround.

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

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

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

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

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

- CSCtu18786

  Symptoms: A device may crash showing “VOIP” error messages. Decodes point to voice functions.

  Conditions: This symptom is observed when SIP is enabled on the device.

  Workaround: There is no workaround.

- CSCtu36224

  Symptoms: A Cisco router reboots unexpectedly at intermittent intervals.

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

Workaround: There is no workaround.

- CSCtw45055

  Symptoms: A Cisco ASR router may experience a crash in the BGP scheduler due to a segmentation fault, if BGP dynamic neighbors have been recently deleted due to link flap. For example:

```
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up
%BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold time expired) x bytes
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification received
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from
session Neighbor deleted
%BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from
session Neighbor deleted
%BGP-5-ADJCHANGE: neighbor *X.X.X.X Up

Exception to IOS Thread:
Frame pointer 0x3BE784F8, PC = 0x104109AC

UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scheduler
```

  The scheduler process will attempt to reference a freed data structure, causing the system to crash.

  Conditions: This symptom is observed when the Cisco ASR router experiences recent dynamic neighbor removals, either because of flapping or potentially by manual removal. This issue only happens when BGP dynamic neighbor is configured.

  Workaround: There is no workaround.

- CSCtw59086

  Symptoms: Connecting via Cisco AnyConnect or the WebVPN portal on a Cisco IOS router fails. The following message is seen in the Syslog:

```
%SSLVPN-6-LICENSE_NO_FREE_COUNT: All available SSLVPN session licenses are in use
```

  Conditions: This symptom is observed when the WebVPN License counter incorrectly reads 4294967295. Also, no connections are visible while executing the **show webvpn session context all** command.

  For example:

```
sh webvpn session context all
show webvpn license
Max platform license count : 1500
Available license count       : 100
Reserved license count       : 100
* In-use count                    : 4294967295*
```

  Workaround: Reload the Cisco router.

- CSCtw76527

  Symptoms: The crypto session stays in UP-NO-IKE state.

  Conditions: This symptom occurs when using EzVPN.

  Workaround: There is no workaround.

- CSCtw98456

  Symptoms: A LAN-to-LAN VPN tunnel fails to come up when initiated from the router side, or when it is up (after being initiated by the peer). Incoming traffic is OK, but no traffic is going out over the tunnel.

Inspection of the IVRF routing table shows that there is a route to the remote destination with the correct next hop, but the route does not point to the egress interface (the interface with the crypto map in the FVRF).

For example, the IVRF routing table should show:

```
S           10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
```

but instead it shows:

```
S           10.0.0.0 [1/0] via 192.168.0.1
```

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

Consequently, no traffic from the IVRF is routed to the egress interface, so no traffic is hitting the crypto map and hence the encryption counters (in **show crypto ipsec sa**) remain at zero.

Conditions: This has been observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 15.1(3)S1. (Cisco IOS Release 15.0(1)S4 has been confirmed not to be affected.) Other IOS versions and other hardware platforms may be affected.

Workaround: Configure a static route to the remote network. For example:

```
ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
```

where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtw99290

  Symptoms: The source or destination group-address gets replaced by another valid group-address.

  Conditions: This symptom is observed during the NVGEN process if it suspends (for example: when having a huge configuration generating the running-config for local viewing or during the saving of the configuration or during the bulk sync with the standby and the NVGEN process suspends). The global shared buffer having the address gets overwritten by another process before the NVGEN completes.

  Workaround: There is no workaround.

- CSCtx29543

  Symptoms: A Cisco router may crash when an IPv4 default route update occurs or when issuing the **show ip route** command.

  Conditions: This symptom occurs under the following conditions:

  1. At least one IPv4 route associated with each of the 23 possible supernet mask lengths exists.
  2. A default route exists.
  3. All routes corresponding to one of the 23 possible supernet mask lengths are removed.

  The router may now crash when issuing the **show ip route** command or when the default route is updated.

  Workaround: There are two possible workarounds:

  1. Ensure that not all 23 supernet mask lengths are populated by doing route filtering.
  2. If workaround #1 is not possible, then ensure that at least one supernet route for all possible mask lengths exists at all times, for example, by configuring summary routes that do not interfere with normal operation.

- CSCtx32628

  Symptoms: When a primary BGP path fails, the prefix does not get removed from the BGP table on the RR/BGP peer although a withdrawal message is received.

  Conditions: This symptom is observed on an L3vpn CE which is dual homed via BGP to a PE under the following conditions:

  - BGP full mesh is configured.
  - BGP cluster-id is configured.
  - **address family vpnv4** is enabled.
  - **address family ipv4 mdt** is enabled.
  - The sending peer is only mcast RD type 2 capable, the receiving peer is MDT SAFI and RD type 2 capable.

  Workaround: Remove the cluster-id configuration or hard-reset the BGP session on the affected Cisco router. However, removing the cluster-id does not guarantee protection.

- CSCtx38806

  Symptoms: SSL VPN users lose connectivity as soon as a 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 a headend 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

- CSCtx77750

  Symptoms: Crosstalk may be heard by PSTN callers when a call is placed on hold and Music on Hold (MMOH) is enabled.

  Conditions: This symptom is observed when CUCM is configured to do Multicast MoH.

  Workaround 1: Disable the H.323 Multicast MoH functionality in Cisco IOS or use SIP Multicast MoH.

  Workaround 2: Use Unicast MoH.

  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 4.3/4.1: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:F/RL:ND/RC:C

  CVE ID CVE-2012-1361 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

- CSCtx88093

  Symptoms: A dialer idle timeout is not initiated after the watched route is installed back in the routing table while using a dialer watch list, causing the watch disconnect timer to not start.

  Conditions: This symptom occurs while using the **dialer-list x protocol ip deny** command to define interesting/uninteresting traffic and while there is traffic flowing over the dialer interface.

  Workaround: Use the method that follows to define interesting traffic instead of the **dialer-list x protocol ip deny** command:

  ```
  access-list x protocol ip deny
  dialer-list 1 protocol ip list x
  ```

- CSCty43587

  Symptoms: Crash observed with memory corruption similar to the following:

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

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

  Workaround: There is no workaround.

- CSCty77190

  Symptoms: DTLS is switched back to TLS after reconnect.

  Conditions: This symptom is observed with the following conditions:

  - Test image: c3845-advsecurityk9-mz.152-2.T1.InternalUseOnly
  - Test version: Cisco IOS Release 15.2(01)T

  Workaround: Restart the AnyConnect client.

- 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.

- CSCty83520

  Symptoms: IP Phone -- CUCM --- H323 -- 3845 - PSTN

  1. A call is originated from the IP phone to a PSTN number and it gets connected.
  2. The IP phone puts the call on hold.
  3. The CUCM instructs GW to listen to the Multicast MoH stream.
  4. The Cisco IOS Gateway sends the RTCP packet to Multicast MoH.

  Conditions: This symptom is observed when the H.323 Gateway is configured and the Multicast MoH and MoH stream is sent across an IP Multicast network.

  Workaround 1: Disable the H.323 Multicast MoH functionality in Cisco IOS.

  Workaround 2: Use Unicast MoH.

- CSCtz27137

  Symptoms: An upgrade to the S640 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.

Resolved Caveats—Cisco IOS Release 15.1(3)T3

Cisco IOS Release 15.1(3)T3 is a rebuild release for Cisco IOS Release 15.1(3)T. The caveats in this section are resolved in Cisco IOS Release 15.1(3)T3 but may be open in previous Cisco IOS releases.

- CSCsh39289

  Symptoms: A router may crash under a certain specific set of events.

  Conditions: The crash may happen under a combination of unlikely events when an IPv6 PIM neighbor that is an assert winner expires.

  Workaround: There is no obvious workaround, but the problem is unlikely to occur.

- CSCso41274

  Symptoms: A router crashes or shows the following traceback:

  ```
  % Not enough DSP resources available to configure ds0-group 1 on controller T1 1/0 %
  The remaining dsp resources are enough for 14 time slots. % For current codec
  complexity, 1 extra dsp(s) are required to create this voice port.
  sip-cme(config-controller)# %ALIGN-3-SPURIOUS: Spurious memory access made at
  0x40C627A8 reading 0x4 %ALIGN-3-TRACE: -Traceback= 0x40C627A8 0x40D6769C 0x40D7281C
  0x40D72E74 0x4036B0E4 0x4036D4B4 0x414C78EC 0x414EB3FC
  ```

  Conditions: The symptom is observed on a router that has enough DSP resources to set up 14 signaling channels. When trying to configure a ds0-group for the 16 time-slot, you may get an error message that not enough DSP resources are available. Immediately after that the router shows the traceback or may crash.

  Example:

  ```
  sip-cme(config)# controller t1 1/0
  sip-cme(config-controller)# ds0-gr 1 time 1-16 type e&m-imm
  sip-cme(config-controller)# ds0-gr 1 time 1-16 type e&m-immediate-start
  ```

  Workaround: Ensure that there are more DSPs in the router than signalling channels.

- CSCta11223

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

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

  Workaround: There is no known workaround.

- 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.

- CSCtd15853

  Symptoms: When removing the VRF configuration on the remote PE, the local PE receives a withdraw message from the remote PE to purge its MDT entry. However, the local PE does not delete the MDT entry.

Conditions:

- mVPN is configured on the PE router.
- Both Pre-MDT SAFI and MDT-SAFI Cisco IOS software is running in a Multicast domain.

Multicast VPN: Multicast Distribution Trees Subaddress Family Identifier:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

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.

- CSCtg68047

  Symptoms: The router reloads.

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

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

- CSCth14305

  Symptoms: Having a bandwidth statement on a multilink bundle interface will cause problems with QoS and BQS if link members flap because the changes in bandwidth will not be handled correctly.

  Conditions: The symptom is observed when you have a bandwidth statement on a multilink bundle.

  Workaround: Avoid bandwidth statements on multilink bundle interfaces.

- CSCth20018

  Symptoms: On a Cisco ISR G2 or Cisco 8xx product line, unconfiguring a subinterface (via config CLI, for example, **no interface g0/0.100** or **no interface atm0/0.100**) may sometimes crash the system.

  Conditions: This symptom occurs during basic configuration.

  Workaround: Do not unconfigure a subinterface.

- CSCth73173

  Symptoms: ASR may crash if a QoS policy applied using CoA through Service-Template is more than 256 characters in length.

  Conditions: This symptom is observed when a QoS Policy string length exceeds 256 characters.

  Workaround: Ensure that the QoS policy string length is less than 256 characters.

- CSCth90147

  Symptoms: Router will respond to an RS with an RA.

  Conditions: The symptom is observed when you configure the **ipv6 nd ra suppress** command. This command is only intended to suppress periodic mcast RAs. The router will still respond to unicast RS (that is intended behavior).

  Workaround: Use an ACL to block the reception of RS packets.

- CSCti01036

  Symptoms: A Cisco ASR 1000 series router crashes on the RADIUS process.

  Conditions: This symptom is observed on a Cisco ASR 1000 series router with RADIUS AAA services enabled. When the RADIUS server sends attributes with no information (empty VSA strings), it produces an unexpected reload on the router.

  Workaround: Prevent the AAA server from sending empty VSA strings.

- CSCti04919

  Symptoms: While unconfiguring and reconfiguring the VRF, PIM neighborship goes down in a specific scenario.

  Conditions: This symptom occurs if the PIM MDT GRE tunnel takes more time to come up compared to other interfaces in the VRF.

  Workaround: Toggle the default MDT.

- CSCti33159

  Symptoms: The PBR topology sometimes chooses a one-hop neighbor to reach a border, as opposed to using the directly-connected link.

  Conditions: This is seen when the border has multiple internal interfaces and one of the internal interfaces is directly connected to a neighbor and the other interface is one hop away.

  Workaround: There is no workaround.

- CSCti64685

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

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

  Workaround: There is no workaround.

- CSCtj21237

  Symptoms: "%SYS-2-LINKED: Bad enqueue, Bad dequeue" messages are received, which might result an in unexpected reboot due to SegV Exception.

  Conditions: The symptom is observed on a router configured with control plane policing and protection feature.

  Workaround: Disable the feature in order to prevent any further crash.

- 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.

- CSCtj56551

  Symptoms: The Cisco 7600 crashes in a very rare case.

  Conditions: This symptom is observed very rarely when route-churn/sessions come up.

  Workaround: There is no workaround.

- CSCtj79769

  Symptoms: LC crashes.

  Conditions: When disabling MLD snooping on an interface or disabling IPV6 multicast in general.

Workaround: There is no workaround.

- CSCtj95685

  Symptoms: A router configured as a voice gateway may crash while processing calls.

  Conditions: The symptom is observed with a router configured as a voice gateway.

  Workaround: There is no workaround.

- CSCtj96915

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

  Conditions: Unknown. See Further Problem Description below.

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

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

- CSCtk00181

  Symptoms: Password aging with crypto configuration fails.

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

  Workaround: There is no workaround.

- CSCtk01638

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

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

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

  Workaround: There is no workaround.

- CSCtk32975

  Symptoms: The system crashes.

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

  Workaround: There is no workaround.

- 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 Cisco 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.

- CSCtl52854

  Symptoms: Client does not receive multicast traffic when it is connected to an EHWIC port in access mode.

  Conditions: The symptom is observed when a multicast server is connected to an EHWIC L2 interface.

  Workaround: Connect the multicast server to an on-board gig interface.

- CSCtl90341

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

  Conditions: This symptom occurs very inconsistently.

  Workaround: There is no workaround.

- CSCtn04357

  Symptoms: When applying the following netflow configuration in the same sequence, the standby supervisor module continuously reloads:

  vlan configuration 161
  ip flow monitor flowmonitor1 in
  ip flow monitor flowmonitor1 input

  Conditions: The symptom is observed on a Sup7-E that is running Cisco IOS XE Release 3.1.0(SG). The router must have a redundant RP. The monitor must be using a flow record that does not conform to V5 export format while being used with V5 exporter and be running on a distributed platform. When the flow monitor is applied to an interface the config sync will fail and the standby will reload.

Workaround 1: Remove the flow monitor configuration.

Workaround 2: Use netflow-v9 export protocol.

Workaround 3: Use a record format exportable by netflow-v5.

- 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.

- CSCtn22728

  Symptoms: See the following:

```
Router(config)# monitor session 1 type erspan-source
Router(config-mon-erspan-src)# destination ?
    <cr>
Router(config-mon-erspan-src)# destination int g11/48
Router(config-if)#
Config Sync: Line-by-Line sync verifying failure on command:
    destination int g11/48
due to parser return error
```

  Conditions: This symptom is seen when using unsupported interface CLI option with destination keyword in ERSPAN source session configuration, which may result in Config-Sync failure between Active and Standby-RP, therefore reloading Standby-RP.

  Workaround: Do not issue not applicable commands.

- CSCtn32323

  Symptoms: 802.1p information is not set on local generated traffic when bridge-dot1q is used on the DSL lines.

  Conditions: Configure the device to transport 802.1p information over a DSL link connection, considering different CoS values for LAN and local generated traffic on the router.

```
interface ATM0.y point-to-point
 bridge-group <x>
 pvc 1/199
  bridge-dot1q encap <vlan>
  service-policy out <egress-policy>
```

  Workaround: There is no workaround.

- CSCtn62287

  Symptoms: The standby router may crash while flapping the interface or while doing soft OIR of the SPA.

  Conditions: This symptom is observed when interfaces are bundled as a multilink and traffic flows across the multilink.

  Workaround: There is no workaround.

- CSCtn68643

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

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

ipv6 ospf encryption ipsec spi 500 esp null sha1 1234123412341234123412341234123412341234

or

ipv6 ospf authentication ipsec spi 500 md5 abcdabcdabcdabcdabcdabcdabcdabcd

Workaround: There is no workaround.

- 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.

- CSCtn74673

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

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

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

- CSCtn83520

  Symptoms: VOIP_RTCP related traceback is seen.

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

  Workaround: There is no workaround.

- 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.

- CSCto14435

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

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

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

- CSCto15371

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

  Conditions: This symptom occurs only when two peers are configured in crypto map and the first peer is unreachable.

  Workaround: Do not use two "set peer" statements in the crypto map definition.

Further Problem Description:

1) Configure 880 to use the software crypto engine.

2) Apply the exact configuration of the UUT to 880. The critical factor is the unreachable peer, which needs to appear before the connected peer.

```
crypto isakmp key cisco address 172.19.152.48 <= Unreachable peer
crypto isakmp key cisco address 192.168.1.104
!
crypto map mymap 1 ipsec-isakmp
  set peer 172.19.152.48 <= Unreachable peer
  set peer 192.168.1.104
  set security-association lifetime seconds 120
  set transform-set TSET3
  match address 101
!
```

3) Once the tunnel is up, ping 880 from the peer continuously.

4) Do a “clear crypto session” on 880.

5) Try to ping the peer from 880.

6) Tracebacks will appear and sometimes the system crashes.

- CSCto39885

  Symptoms: A router crashes.

  Conditions: gcid and callmon is turned on.

  Workaround: There is no workaround.

- CSCto48060

  Symptoms: A Cisco 3900 series router may crash with the following error:

  ```
  Unexpected exception to CPU: vector 1400
  ```

  Conditions: The symptom is observed when the router is configured as a voice gateway using H323 and H245 and connected to CUCM. If CUCM is sending a MultiMediaSystemControl messages with no entry, the router may crash.

  Workaround: There is no workaround.

- CSCto55643

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

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

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

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

- CSCto55983

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

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

Workaround: There is no workaround.

- 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.

- CSCto63268

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

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

  Workaround: Remove the EVM or disable DSP sharing.

- CSCto72480

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

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

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

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

- CSCto72927

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

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

  Workaround: None.

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

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

  No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

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

- CSCto73345

  Symptoms: A router crashes while reloading after configuring a crypto IPsec manual keying policy.

Conditions: This issue is seen when a router that is configured with a crypto IPsec manual keying policy is reloaded.

Workaround: There is no workaround.

- CSCto86833

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

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

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

- CSCto88393

  Symptoms: CPU hogs are observed on a master controller:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (0/0),process
  = OER Master Controller.
  ```

  Conditions: This symptom is observed when the master controller is configured to learn 10,000 prefixes per learn cycle.

  Workaround: There is no workaround.

- CSCto89536

  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

- CSCtq12007

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

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

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

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

- CSCtq21234

  Symptoms: Label is not freed.

  Conditions: The symptom is observed after shutting down the link.

  Workaround: There is no workaround.

- CSCtq24733

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

  Conditions: The symptom is observed with MRCP is enabled.

  Workaround: There is no workaround.

- CSCtq25682

  Symptoms: The router crashes after configuring “gw-accounting file”.

  Conditions: This symptom occurs if the router’s memory usage is already over 80 percent utilization, and after configuring “gw-accounting file”, the following log message is displayed:

  ```
  %VOICE_FILE_ACCT-4-MEM_USAGE_HI_WATERMARK: System memory on high usage (81/100).
  Stopping processing new event log for now.
  ```

  After this log, when the cdrflush-timer expires, the router crashes.

  Workaround: Do not enable “gw-accounting file” when the router’s memory utilization is already over 80 percent.

- CSCtq26892

  Symptoms: CUBE crashes @ sipSPI_ipip_IsHdrInHeaderList.

  Conditions: This symptom is observed with a PRACK-NO PRACK configuration on Cisco IOS Release 15.2(1)T.

  Workaround: There is no workaround.

- CSCtq32896

  Symptoms: LSM entries stop forwarding traffic.

  Conditions: This symptom is observed after Stateful Switchover (SSO).

  Workaround: There is no workaround.

- CSCtq36153

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

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

  Workarounds that mitigate these vulnerabilities are not available.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is available at the following link:

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

- 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

- CSCtq47428

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

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

  Workaround: There is no workaround.

- CSCtq49325

  Symptoms: A router reloads when a graceful shutdown is done on EIGRP.

  Conditions: The router reload occurs only when multiple EIGRP processes redistributing each other run on two redundant LANs and a graceful shutdown is done on both EIGRP processes simultaneously.

  Workaround: Redundant LANs may not be necessary in first place. If it is required, if mutual redistribution is done, then while doing graceful shutdown, sufficient time should be given for one process to be shutdown completely before executing the second shutdown command. This should resolve the problem.

  Further Problem Description: In a normal scenario, a zombie DRDB or path entry (a temporary DRDB entry which is deleted as soon as processing of the packet is done) would be created only for reply message. But here, due to the redundancy in LAN and EIGRP processes in this scenario, a query sent on one interface comes back on the other which causes this zombie entry creation for the query also. In the query function flow it is expected that this zombie entry will not be deleted immediately, rather it is to be deleted only after a reply for the query is sent successfully. At this point, (i.e.: before a reply is sent) if a shutdown is executed on the EIGRP process, then all the paths and prefixes will be deleted. However if a particular path is threaded to be sent, in this case it is scheduled for a reply message, the path is not deleted and an error message is printed. However the flow continues and the prefix itself is deleted. This results in a dangling path without the existence of any prefix entry. Now when the neighbors are deleted, the flushing of the packets to be sent will lead to crash since it does not find the prefix corresponding to the path. The solution is to unthread from the paths from sending before deletion. A similar condition will occur if the packetization timer expiry is not kicked in immediately to send the DRDBs threaded to be sent and a topology shutdown flow comes to execute first.

- 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.

- CSCtq56727

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

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

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

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

  Workaround: There are two workarounds:

  1. Set the DTMF signaling type as “OOB and RFC 2833” in the Communications Manager SIP trunk configuration that is pointing to the SIP gateway.

  2. Configure “dtmf-relay rtp-nte” (instead of “sip-kpml”) in the SIP gateway dial-peer configuration. The Unified Communications Manager is configured with “no preference.”

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

- CSCtq58383

  Symptoms: A crash occurs when modifying or unconfiguring a loopback interface.

  Conditions: This symptom occurs while attempting to delete the loopback interface, after unconfiguring the “address-family ipv4 mdt” section in BGP.

  Workaround: Unconfiguring BGP may prevent the issue from happening without reloading the router.

- CSCtq61128

  Symptoms: Router is crashing with Segmentation fault(11)

  Conditions: It was observed on routers acting as IPSEC hub using certificates.

  Workaround: None.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.3/5.2:

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

  CVE ID CVE-2011-4231 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

- CSCtq75008

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

  Conditions:

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

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

  Workaround: There is no workaround.

- CSCtq80648

  Symptoms: If a user changes the VRF assignment, such as moving to another VRF, removing the VRF assignment, etc., on which a BGP ipv6 link-local peering (neighbor) is based, the BGP IPv6 link-local peering will no longer be able to delete or modify.

  For example:

```
interface Ethernet1/0
  vrf forwarding vpn1
    ipv6 address 1::1/64
!
router bgp 65000
  address-family ipv6 vrf vpn1
    neighbor FE80::A8BB:CCFF:FE03:2200%Ethernet1/0 remote-as 65001
```

  If the user changes the VRF assignment of Ethernet1/0 from vpn1 to vpn2, the IPv6 link-local neighbor, FE80::A8BB:CCFF:FE03:2200%Ethernet1/0, under address-family ipv6 vrf vpn1, will no longer be able to delete or modify.

  Rebooting the router will reject this configuration. Also, if a redundant RP system and the release support config-sync matching feature, it will cause config-sync mismatch and standby continuous reload.

  Conditions: This symptom occurs when a user changes the VRF assignment.

  Workaround: Remove the BGP IPv6 link-local peering before changing the VRF assignment on the interface.

- CSCtq83629

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

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

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

- CSCtq85728

  Symptoms: An EHWIC-D-8ESG card is causing an STP loop.

  Conditions: EHWIC-D-8ESG might not be blocking appropriate ports according to calculated STP topology that introduces the loop in the network.

  Workaround: There is no workaround.

- CSCtq88777

  Symptoms: VDSL controller and ATM interface remains up, however ATM PVC becomes inactive and virtual interface goes down.

  Conditions: The symptom is observed when the ATM PVC becomes inactive causing the virtual interface to go down.

  Workaround: Use a VBR-NRT value that is lower than trained upstream speed.

- 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.

- CSCtq97991

  Symptoms: ADSL interface fails to re-train when “dsl enable-training-log” is configured.

  Conditions:

  1. Observed in a Cisco 800, 1900, and 2900 chassis and could affect other software platforms.

  2. Observed in Cisco IOS Release 15.1(2)T, Release 15.1(2)T1, and Release 15.1 (3)T. 3. It is not observed in Cisco IOS Release 15.0(1)M4.

  Deviation observed in the following manner:

  1. With “dsl enable-training log” not configured the HWIC trains up to the DSLAM OK. After unplugging cable and reconnecting it, the HWIC still comes up fine after.

  2. Configure “dsl enable-training log”. After unplugging cable and reconnecting it, the HWIC fails to come up. CD LED does not blink and the following error message appears: “No retrain. sleep 20 seconds”.

  Workaround: Remove “dsl enable-training-log.”

- CSCtr04829

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

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

  Workaround: There is no workaround.

- CSCtr06747

  Symptoms: ISIS neighborship remains in INIT state when MTU at both ends is changed to 4470.

  Conditions: The symptom is observed when a Cisco 2900 is used in the topology with MTU 4470 (any MTU > 2000).

  Workaround: Replace the Cisco 2900 with a Cisco 2800 or reduce the MTU to < 2000.

- CSCtr11620

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

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

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

- 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.

- CSCtr18574

  Symptoms: H323-H323 video calls fail with cause code 47.

  Conditions: The symptom is observed when an H323-H323 video call fails to establish an H245 media connection. The following errors are seen:

```
Received event H225_EV_H245_FAILED while at state H225_WAIT_FOR_H245
cch323_send_passthru_out: Send passthru message retcode 15
```

Workaround: There is no workaround.

- CSCtr25821

  Symptoms: A Cisco 800 series router crashes with **isdn leased-line bri*0* 128** command:

  ```
  Unexpected exception to CPU: vector 1000, PC = 0x0 , LR = 0x8155A310
  ```

  Conditions: The symptom is observed with the **isdn leased-line bri0 128** command.

  Workaround: The issue does not occur if there is no cable that connects to the BRI interface. Disconnect the cable from the BRI interface while the **isdn leased-line bri0 128** command is configured.

- 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 a "%ISDN-6-DISCONNECT" message from "unknown" followed by a couple of "Illegal Access to Low Address" messages.

  Workaround: There is no workaround.

- CSCtr44686

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

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

  Conditions: The symptom is observed with the above maps.

  Workaround: Replace "reset" with "log".

- CSCtr45608

  Symptoms: Referring an IPv6-only VRF on a route-map crashes the router.

  Conditions: The symptom is observed on a Cisco Catalyst 4000 Series Switch when "set vrf" is configured on the route-map and the VRF is IPv6 only.

  Workaround: Configure "ipv4 vrf" along with "ipv6 vrf" and refer "ipv6 vrf" on the route-map by configuring "ipv6 policy" on the ingress interface.

- CSCtr46123

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

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

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

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

- CSCtr49064

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

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

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

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

- CSCtr51926

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

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

  Workaround 1: Enable IPv6 explicitly on the main interface:

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

  Workaround 2: Reconfigure the IPv6 address on the subinterface:

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

- CSCtr54269

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

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

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

- CSCtr54327

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

  Conditions: The crash occurs on a voice gateway that is configured with transcoding and fax passthrough where a fax call comes in for a codec, but the fax is not configured for a codec, and the “a=silenceSupp:off” option is set in SDP.

  Workaround: There is no workaround.

- CSCtr58140

  Symptoms: PFR-controlled EIGRP route goes into Stuck-In-Active state and resets the neighbor.

  Conditions: This symptom is observed when the PFR inject route in an EIGRP topology table after the policy decision. The issue was first seen on an MC/BR router running PFR EIGRP route control and with EIGRP neighbors over GRE tunnels.

  Workaround: There is no workaround.

- CSCtr79347

  Symptoms: A Cisco ASR1006 crashes without a BGP configuration change or BGP neighbor up/down event.

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Task
  ```

  ```
  Traceback summary % 0x80e7b6 : __be_bgp_tx_walker_process % 0x80e3bc :
  __be_bgp_tx_generate_updates_task % 0x7f8891 : __be_bgp_task_scheduler
  ```

  Conditions: No conditions but this is a rarely observed issue.

  Workaround: There is no workaround.

- CSCtr86437

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

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

  Workaround: Reconfigure “ipv6 nat prefix.”

- CSCtr91106

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

  This advisory is available at the following link:

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

- CSCtr92779

  Symptoms: Call scenario is with Avaya CM6 over TLS/SIP trunks, which causes the Cisco 3945 router (running Cisco IOS Release 15.1(4)M1) CUBE to crash.

  Conditions: The symptom is observed when a call is originated from Cisco Phone A via TLS/SIP Trunk to CUBE (3945 15.1(4)M1) to Avaya CM6 Phone A, which is set to “call forward all” back to the original Cisco Phone A.

  Workaround: There is no workaround.

- 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

- CSCts06929

  Symptoms: Disposition traffic gets dropped after SSO as the new local labels allocated by AToM do not get programmed on the line cards.

  Conditions: This symptom occurs when pseudowires are configured on the setup without graceful restart configured. Then, SSO is performed and two local labels have the same disposition information. This really manifests as a traffic drop issue when the scale is high.

  Workaround: Configuring graceful restart resolves this issue.

- CSCts16285

  Symptoms: The system may experience delays in updating multicast information on the line cards. MFIB/MRIB error messages may be observed when IPC messages from the line card to the RP time out. In the worst case, the line card may become disconnected if timeouts continue for a long period.

  Conditions: This symptom occurs when the system has a very heavy IPC load or CPU load.

  Workaround: Take necessary actions, if possible, to reduce the IPC load. Sometimes, the IPC load could be due to noncritical processes.

- CSCts28315

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

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

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

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

  Workaround: There is no workaround.

- CSCts33952

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

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

  Workaround: There is no workaround.

- 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

- CSCts39535

  Symptoms: BGP IPv6 routes that originate from the local router (via network statements or redistribute commands) fail to match any specified condition in an outbound route map used on a neighbor statement, regardless of the expected matching results. Thus, the route map may not be applied correctly, resulting in erroneous filtering or advertising of unintended routes.

  Further testing revealed that the “suppress-map” and “unsuppress-map” commands (used in conjunction with the “aggregate-address” command) are also broken, in the sense that the route-map filtering will fail to correctly suppress or unsuppress a subnet under the aggregated prefix.

  Conditions: An outbound route map with a match statement is used in a “neighbor” statement for an IPv6 or VPNv6 neighbor in BGP, and there are locally originated routes, either through network statements or by redistribution. All “match” statements except for “as-path”, “community,” and “extcommunity” are impacted; this includes match ipv6 address, protocol, next-hop, route-source, route-type, mpls, tag.

  Workaround: None for the same router. However, inbound route maps work fine, so configuring inbound route maps on the neighboring router can compensate.

  Another way to handle it would be to configure prefix lists directly on the network statement. So filtering will be preserved. But, there will not be a way to “set” anything as route maps can typically do.

- CSCts40771

  Symptoms: Device goes into a hang state and requires a power cycle. If “scheduler isr-watchdog” is configured, the device will crash and reload the system.

  Conditions: This issue has been seen with “ip nbar protocol-discovery” configured on tunnel interfaces.

  Workaround: Remove “ip nbar protocol-discovery” from the device.

- 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.

- CSCts64539

  Symptoms: The BGP next hop is inaccessible. The **show ip route** command output in the global and VRF routing tables shows that the next hop is reachable. The **show ip bgp vpnv4 all attr next-hop** command output shows max metric for the next hop.

  Conditions: This symptom occurs when an import map uses the “ip vrf name next-hop” feature while importing single-hop eBGP routes from the global routing table to the VRF routing table.

  Workaround 1: If “set ip next-hop” is not configured in import route map, this issue does not occur.

  Workaround 2: If “neighbor x.x.x.x ebgp-multihop” is configured, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

  Workaround 3: If “neighbor x.x.x.x diable-connected-check” is configured for a single-hop eBGP, this issue does not occur. The knob needs to be configured for all eBGP peers, where routes are imported to the VRF with “set ip next-hop”.

- 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.

- CSCts78348

  Symptoms: Packet drop will occur on a router when the interface is configured as 10/full.

  Conditions: It seems that when interface is configured as 10/full, with the traffic of 10 Mbps, this issue will occur. By performing a shut/no shut on the interface, this issue will recover but it will be seen again when you reload the device.

  This issue may be seen on a Cisco 19xx and a Cisco 29xx (except Cisco 2951) This issue may occur when manual set duplex on the affected platform.

  Workaround 1: Perform a shut/no shut on the interface and this issue will recover.

  Workaround 2: Use auto negotiation.

- CSCts80643

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

  A workaround is available to mitigate this vulnerability.

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

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

- CSCtt11210

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

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

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

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

- CSCtt16051

  Cisco IOS Software contains a vulnerability in the Smart Install feature that could allow an unauthenticated, remote attacker to cause a reload of an affected device if the Smart Install feature is enabled. The vulnerability is triggered when an affected device processes a malformed Smart Install message on TCP port 4786.

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

  This advisory is available at the following link:

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

- CSCtt17879

  Symptoms: The **bgp network backdoor** command does not have any effect.

  Conditions: This symptom occurs:

  - On 64-bit platform systems.
  - When the network is learned after the backdoor has been configured.

  Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt20215

  Symptoms: Controller goes down after reload.

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

  Workaround: Unplug/plug the cable, or reset link from PBX side.

- CSCtt96597

  Symptoms: Unable to power-cycle modem using **test cellular** *unit* **modem-power-cycle**.

  Conditions: The symptom is observed when a router cannot communicate with the modem due to a possible modem firmware crash or device disconnect.

  Workaround: Reload router.

- CSCtt98801

  Symptoms: Mobile router reports stale RRP received from HA.

  Conditions: The symptom is observed when the mobile router sends a RRQ to HA in CCOA mode.

  Workaround: There is no workaround.

- CSCtu07626

  Symptoms: Router processing SIP traffic crashes.

  Conditions: The following error may be seen prior to the crash:

  ```
  %SDP-3-SDP_PTR_ERROR: Received invalid SDP pointer from application. Unable to
  process.
  ```

  Workaround: There is no workaround.

- CSCtw67599

  Symptoms: IPsec tunnels do not come up.

  Conditions: This symptom is observed in Cisco IOS Release 15.1(3)T2.3, which uses a hardware crypto engine.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(3)T2

Cisco IOS Release 15.1(3)T2 is a rebuild release for Cisco IOS Release 15.1(3)T. The caveats in this section are resolved in Cisco IOS Release 15.1(3)T2 but may be open in previous Cisco IOS releases.

- 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.

- CSCtb24959

  Symptoms: The router may crash while clearing a large number of RP mappings.

  Conditions: This symptom occurs when you configure the router as an RP agent and candidate RP for a large number of RPs. This issue is seen when you run the **clear ip pim rp-map** command several times.

  Workaround: Do not run the **clear ip pim rp-map** command several times in succession.

- 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.

- CSCtd23069

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

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

  Workaround: There is no workaround.

- 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. This issue is seen with Cisco IOS Release 12.4(24)T1 or Cisco IOS Release 12.4(24)T2.

  Workaround: There is no workaround.

- CSCtf39056

  Symptoms: RRI route will not be deleted even after IPSec SA has been deleted.

  Conditions: This symptom was first observed on the Cisco ASR1k running Cisco IOS Release 12.2(33)XND, but is not exclusive to it. The conditions are still under investigation.

  Workaround: Reload the router to alleviate this symptom temporarily. One possible workaround would be to set up an EEM script to reload the device at night. In this case, the reload should occur at 3:00 a.m. (0300) in the morning. For example (the syntax may vary depending on the versions used):

```
############
configure terminal
!
event manager applet SR_000000526
event timer cron name SR_000000526 cron-entry "0 3 * * *"
action 1 cli command "en"
action 2 cli command "reload"
!
end
############
```

- CSCtg54878

  Symptoms: Static routes with only the name option are not installed in the route table.

```
Router(config)#ip route <des ip add> <sub mask> <ip add> name test track
101
                                                                  ^^^^^^
                                                                 name option

Router#sh runn | sec track
    ip route <des ip add> <sub mask> <ip add> name test track 101

Router#show ip route track
      ==> ip route <des ip add> <sub mask> <ip add> name test track 101 is
not installed
```

Conditions: This symptom is observed with static routes that have only the name option.

Workaround: Instead of using ip route <des ip add> <sub mask> <ip add> name test track, use the following:

```
ip route <des ip add> <sub mask> <ip add> intf track name test
```

For example:

```
ip route 1.1.1.1 255.255.255.255 e0/0 track 1 name abc
```

- CSCtg72652

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

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

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

  Workaround: There is no workaround.

- CSCtg84969

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

  Conditions: The symptom is observed on a dual RP Cisco 7600 series router with line cards after multiple reloads or SSOs. When the issue occurs, the output of **show ip mfib vrf** *vrf-name* **verbose** on the standby SP will show some lines preceeded with "###" where an interface name is expected.

  Workaround: There is no workaround.

- CSCtg89555

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

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

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

- CSCth01526

  Symptoms: The MDT interface is deactivated and activated after an SSO.

  Conditions: This symptom is observed after an SSO, when the PIM register tunnel or MDT tunnel may go down briefly on switching to the standby RP.

  Workaround: There is no workaround.

- CSCth11006

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCth85294

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

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

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

- CSCth87458

  Symptoms: Memory leak is detected in ssh_buffer_get_string.

  Conditions: Use test tool Codenomicon to test SSH verification against UUT (SSH-Server test). After the test, the memory leak will be seen in ssh_buffer_get_string.

  Workaround: There is no workaround.

- CSCti18615

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

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

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

- CSCti25459

  Symptoms: The device might crash with fib_forw_add_extra_encap_and_forward. Also, possibly ICMP packets with unreachable sourced may be seen.

  Conditions: This symptom is observed when MLPS is enabled on these devices.

  Workaround: Use NAT NVI instead of legacy NAT.

- CSCti40660

  Symptoms: The following message is displayed:

  ```
  %FW-4-GLOBAL_SESSIONS_MAXIMUM: Number of sessions for the firewall exceeds the
  configured global sessions maximum value 2147483647
  ```

  Conditions: This symptom is observed when IP SLA is configured along with self zones.

  Workaround: There is no workaround.

- 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.

- CSCtj04672

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

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

- CSCtj05903

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

  Conditions: This symptom occurs on scaled sessions.

  Workaround: There is no workaround.

- CSCtj15090

  Symptoms: The IPv6 connection setup between Cisco IOS Release 12.4 and Cisco IOS Release 12.2 fails.

  Conditions: This symptom occurs when the Sender (or responder) is running Cisco IOS Release 12.4 and the Responder (or sender) is running Cisco IOS Release 12.2. Because of a message mismatch, the control message for IPv6 fails.

  Workaround: Use “control disabled”, as there is no workaround if control is enabled.

- CSCtj23189

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

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

  Workaround: There is no workaround.

- CSCtj33003

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

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

  This advisory is available at the following link:

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

- CSCtj36521

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

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

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

- CSCtj84234

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

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

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

  Workaround: There is no workaround.

- CSCtj87846

  Symptoms: Performance Routing (PfR) traffic class fails to transition out of the default state.

  Conditions: When a subinterface is used as an external interface and the corresponding physical interface goes down and comes up, the PfR master is not notified that the subinterface is a backup.

  Workaround: Do shut/no shut on PfR master or PfR border.

- CSCtk02814

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

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

  Workaround: There is no workaround.

- CSCtk12681

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

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

  Workaround: Disable IP SLA TRACE for VoIP RTP probe.

- CSCtk18607

  Symptoms: The router crashes at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

  Conditions: This symptom occurs at ssh_pubkey_command_nvgen and ssh_pubkey_nvgen.

  Workaround: There is no workaround.

- CSCtk31401

  Symptoms: A Cisco router crashes when the SSH session from it is exited.

  Conditions: This symptom is observed when “aaa authentication banner” is configured on the router.

  Workaround: There is no workaround.

- CSCtk36891

  Symptoms: Video conferencing through NAT may crash the router.

  Conditions: This symptom occurs when NAT is configured to perform ALG processing on SKINNY messages. As a result, video conferencing with PVDM3 crashes the router.

  Workaround: Disable NAT ALG processing of SKINNY messages using the **no ip nat service tcp** *port* command, where *port* is the port number used by the SKINNY protocol. The default SKINNY port is 2000. So, if SKINNY is using the default port, then the command would be “no ip nat service tcp port 2000”.

- CSCtk52807

  Symptoms: Processor pool memory corruption crash is observed.

  Conditions: This condition occurs when VoIP/SIP is enabled.

  Workaround: Upgrade the phone load to SCCP42.9-1-1SR1S or later and decrease hunt group timeouts.

- CSCtk62950

  Symptoms: SSH over IPv6 may crash the router.

  Conditions: This symptom occurs with SSH over IPv6.

  Workaround: There is no workaround.

- CSCtk67073

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCtk68647

  Symptoms: The Cisco ASR is configured as a DMVPN hub and spoke connections fail to rekey or initially connect after the box has been up for some time. The length of time is based on the number of connections. In addition, the **show crypto sockets** command output shows that sockets are leaking and do not release even when the SA is inactive.

  Conditions: This symptom is observed with the Cisco ASR code prior to Cisco IOS XE Release 3.2.0. This issue is seen with multiple DMVPN tunnels configured with tunnel protection and the **shared** keyword.

Workaround: Upgrade the Cisco ASR code to Cisco IOS XE Release 3.2.0. Remove other DMVPN tunnels (or shut them down).

- CSCtk74660

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

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

  Workaround: There is no workaround.

- CSCtk98021

  Symptoms: Portions of the WebVPN/SSL VPN code in the Cisco IOS needs to be enhanced to address secure coding best practices.

  Conditions: This symptom occurs with a Cisco IOS device configured for WebVPN/SSL VPN.

  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 5.4/4.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:POC/RL:U/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

- CSCtl00467

  Symptoms: A Cisco router crashes.

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

  Workaround: There is no workaround.

- CSCtl05684

  Symptoms: Xauth user information remains in the **show crypto session summary** command output.

  Conditions: This symptom is observed when running EzVPN and if Xauth is performed by a different username during P1 rekey. This issue is seen when NAT is used in the VPN path.

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

- CSCtl20509

  Symptoms: In CME/SRST 4.0, when ATA unregister/fall back to the Cisco Unified CallManager, the virtual POTS dial peers stay up and calls to ATA do not go out the H323 dial peer to the 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 peers for the ATA are up.

  Workaround: Reload the router.

- CSCtl43156

  Symptoms: When using a BVI interface configured for IPv6 on a Cisco ISR-G2 series router, IPv6 neighbors are never discovered over the BVI. Neighbors will never be seen in the **show ipv6 neighbors** command output and all traffic to/through the BVI will fail.

Conditions: This symptom occurs when IPv6 is configured on Cisco ISR-G2 router images running on the “datak9” package.

Workaround: Use the “uck9” technology package, where the IPv6 feature is already present.

- CSCtl45684

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

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

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

  Workaround: There is no workaround.

- CSCtl53899

  Symptoms: SIP to SIP calls through CUBE may cause memory corruption when resource priority passthrough is enabled on the dial peers.

  Conditions: This symptom is observed on CUBE with Cisco IOS Release 15.1(3)T, where the following was configured under the SIP dial peers:

  ```
  voice-class sip resource priority mode passthrough
  ```

  Workaround: Disable memory lite allocations using the **no memory lite** command. This will increase the size of memory allocations, so be careful when using it on a device with high memory utilization.

- CSCtl67079

  Symptoms: The following error message is seen on a Cisco router with HWIC_1GE_SFP inserted:

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

  Conditions: This symptom is observed during bootup.

  Workaround: There is no workaround.

- CSCtl94813

  Symptoms: When using iLBC, the VG224 fails to play audio out the FXS port. The call uses iLBC when the analog phone on the VG224 attends a conference bridge. It causes one-way audio.

  - When the IP capture is decoded from the VG224, the iLBC audio packet received and sent to the VG224 Fast Ethernet interface is clearly seen.
  - For the same call, the PCM trace shows no audio in the RIN stream.

  Conditions: This symptom occurs with Cisco IOS Release 15.1(2)17T. As per the HPI logs, the Cisco IOS does not send any packets to the dsp:

  ```
  *Mar 10 23:36:54.988: //1944/9948BD1D87E7/HPI/[0/1:1]/hpi_receive_query_rx:
     Got RX stats
     Packet details:
      Packet Length=188, Channel Id=1, Packet Id=200
      RX Packets=0: Signaling=0, ComfortNoise=0
      Receive Duration=129180(ms): Voice=0(ms), FAX=0(ms)
      Packet Counts: OOSequence=0, Bad header=0, Late=0, Early=0Receive
  inactive duration=129(ms)
  ```

  Workaround: Downgrade the Cisco IOS to Cisco IOS Release 12.4(4)T8.

- CSCtl95752

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

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

  Workaround: There is no workaround.

- CSCtl98132

  Symptoms: XDR CPU hog may cause system crash.

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

  Workaround: There is no workaround.

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

- CSCtn04686

  Symptoms: When MHSRP is configured and the hello packets are passing through Etherchannel, and the cables connected to the Etherchannel port are unlugged/plugged, the MHSRP hello packets are not received on the Etherchannel interface.

  Conditions: This symptom is observed on a Cisco 3845 router running Cisco IOS Release 15.0(1)M4.

  Workaround: Unplug/plug the cables.

- 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.

- CSCtn08258

  Symptoms: The router crashes.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(2)T2 and Cisco IOS Release 15.1(3)T1 when SIP calls are made.

  Workaround: There is no workaround. However, this issue is not seen in Cisco IOS Release 15.1(4)M.

- CSCtn10922

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

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

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

- CSCtn12119

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

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

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

- CSCtn19178

  Symptoms: If you are running an Inter-AS MPLS design across two autonomous systems, the router may clear the local label for a working vrf "A" and a new local label will not be reassigned.

  Conditions: This symptom occurs on the MPLS Edge LSR when you remove the configuration of an unused vrf "B", including:

  – The vrf interface, for example, **no interface Gi1/0/1.430**.

  – The same vrf process, for example, **no router ospf** *process id* vrf *vrf name*.

  Run the following commands to verify whether you are facing this issue:

  – **show ip bgp vpnv4 vrf A** *subnet* (this is for the working vrf)

  – **show mpls forwarding-table labels** *local label*

  Workaround: To reprogram a new local label on the PE router, clear the MP-BGP session by using either of the following commands:

  – **clear ip bgp** *mp-bgp neighbor* **soft in**

  – **clear ip bgp** *mp-bgp neighbor* **soft out**

- 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.

- CSCtn26785

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

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

  3845#sh cef int atm 1/0
  ATM1/0 is up (if_number 5)
      Corresponding hwidb fast_if_number 5
      Corresponding hwidb firstsw->if_number 5
      Internet address is 64.65.248.174/30
      ICMP redirects are never sent
      Per packet load-sharing is disabled
      IP unicast RPF check is disabled
      Input features: Ingress-NetFlow
      Output features: Post-Ingress-NetFlow
  ```

```
    IP policy routing is disabled
    BGP based policy accounting on input is disabled
    BGP based policy accounting on output is disabled
    Hardware idb is ATM1/0
    Fast switching type 9, interface type 138
    IP CEF switching enabled
    IP CEF switching turbo vector
    IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
    Input fast flags 0x0, Output fast flags 0x0
    ifindex 5(5)
    Slot Slot unit 0 VC -1
    IP MTU 4470
3845#
```

Conditions: The conditions are unknown at this time.

Workaround: There is no workaround.

- CSCtn38996

  Symptoms: All MVPN traffic is getting blackholed when a peer is reachable using a TE tunnel, and an interface flap is done so that the secondary path can be selected. The multicast route does not contain a native path using the physical interface.

  Conditions: This symptom is seen when **mpls traffic-eng multicast-intact** is configured under OSPF.

  Workaround: Issue the **clear ip ospf process** command on the core router.

- CSCtn48744

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

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

  Workaround: There is no workaround.

- CSCtn53094

  Symptoms: The router crashes or generates the following error:

  ```
  %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 8796350. -Process=
  "Mwheel Process", ipl= 2, pid= 315
  ```

  Conditions: This symptom is observed when toggling very fast between the **ip pim** *mode* and **no ip pim** commands on an interface when that interface is the only one where PIM is being enabled. The most common way this can happen in a production network is through the use of “config replace”, which results in the toggling of the command from ON to OFF and then ON on a different interface.

  Workaround: Avoid fast toggling of the **pim** *mode* command if possible when it is only present on a single interface.

- CSCtn58128

  Symptoms: The BGP process in a Cisco ASR 1000 router that is being used as a route reflector may restart with a watchdog timeout message.

  Conditions: This symptom may be triggered by route-flaps in scaled scenario, where the route reflector may have 4000 route reflector clients and processing one million+ routes.

  Workaround: Ensure that “no logging console” is configured.

- CSCtn65060

  Symptoms: A Cisco device crashes.

Conditions: This symptom is observed with Cisco IOS Release 15.0M and Cisco IOS 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.

- CSCtn69929

  Symptoms: The DHCP server does not assign any addresses to clients, even though smart-install is configured with DHCP pool parameters.

  Conditions: This symptom occurs when smart-install is configured to assign DHCP addresses.

  Workaround: Execute the **show running-configuration** command on the box once.

- CSCtn72939

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

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

  Workaround: Configure bridge-group under that xconnect interface.

- 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

- 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.

- CSCtn91807

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

  Conditions: This symptom occurs when a button is pressed on a phone while using skinny. However, the exact conditions that cause this symptom are currently unknown.

  Workaround: There is no workaround.

- CSCtn93891

  Symptoms: Multicast traffic is getting blocked.

  Conditions: This symptom occurs after SSO with mLDP and P2MP-TE configurations.

  Workaround: There is no workaround.

- CSCtn96521

  Symptoms: When the Spoke (dynamic) peer group is configured before the iBGP (static) peer group, the two iBGP (static) neighbors fail to establish adjacency.

  Conditions: This symptom is observed when the Spoke (dynamic) peer group is configured before the iBGP (static) peer group.

Workaround: If the order of creation is flipped, the two iBGP (static) neighbors will establish adjacency.

- CSCtn97451

  Symptoms: The bgp peer router crashes after executing the **clear bgp ipv4 unicast** *peer* command on the router.

  Conditions: This symptom occurs with the following conditions:

```
Router3 ---ebgp--- Router1 ---ibgp--- Router2

ROUTER1:
--------
interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
  ip pim sparse-mode
!

router ospf 100
  network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1 bgp log-neighbor-changes
  network 0.0.0.0
  neighbor 10.1.1.2 remote-as 1
  neighbor 10.1.1.3 remote-as 11
!

ROUTER2:
--------
interface Ethernet0/0
  ip address 10.1.1.2 255.255.255.0
  ip pim sparse-mode
!
router ospf 100
  redistribute static
  network 0.0.0.0 255.255.255.255 area 0
!
router bgp 1
  bgp log-neighbor-changes
  network 0.0.0.0
  redistribute static
  neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4

ROUTER3:
-------
interface Ethernet0/0
  ip address 10.1.1.3 255.255.255.0
  ip pim sparse-mode
!
router bgp 11
bgp log-neighbor-changes
  network 0.0.0.0
  network 0.0.0.0 mask 255.255.255.0
  redistribute static
  neighbor 10.1.1.1 remote-as 1
!
ip route 192.168.0.0 255.255.0.0 10.1.1.4
```

  Crash reproduce steps are as follows:

  1. Traffic travel from ROUTER3 to ROUTER2.

2. "clear bgp ipv4 unicast 10.1.1.1" on ROUTER2.

Workaround: There is no workaround.

- CSCto00318

  Symptoms: SSH session that is initiated from a router that is running Cisco IOS Release 15.x may cause the router to reboot.

  For now, consider not initiating a SSH session from the Cisco router that is running a Cisco IOS Release 15.x train.

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 15.x.

  Workaround: There is no workaround.

- CSCto00796

  Symptoms: In a rare and still unreproducible case, the RR (also PE) misses sending RT extended community for one of the redistributed vpnv4 prefix to the PE (also and RR) that is part of a peer-group of PE (+RR).

  Conditions: This symptom occurs when a new interface is provisioned inside a VRF and the configuration such that the connected routes are redistributed in the VRF. This redistributed route fails to tag itself with the RT when it reaches the peering PE (+RR)

  Workaround: Soft clear the peer that missed getting the RT.

- CSCto02448

  Symptoms: On doing an inbound route refresh, the AS-PATH attribute is lost.

  Conditions: This symptom is observed with the following conditions:

  1. The neighbor is configured with soft-reconfiguration inbound.
  2. The inbound routemap is not configured for the neighbor.
  3. The non-routemap inbound policy (filter-list) allows the path.

  Workaround: Instead of using the non-routemap inbound policy, use the routemap inbound policy to filter the prefixes.

- CSCto03446

  Symptoms: When a flat bandwidth policy is attached to a serial subinterface via frame-relay map-class, all packets are dropped and no traffic goes through.

  Conditions: This symptom occurs with a flat policy attached to frame-relay interface with traffic shaping enabled.

  Workaround: Remove traffic shaping from the interface and attach a hierarchical policy.

- CSCto07586

  Symptoms: An IPV4 static BFD session does not get established on a system which does not have IPV6 enabled.

  Conditions: This symptom occurs with the following conditions:

  1. Create an IOS image that does not IPV6 enabled.
  2. Enable BFD on an interface.
  3. Configure an IPV4 static route with BFD routing through the above interface.

  The IPV4 BFD session does not get established, so the static route does not get installed.

  Workaround: Unconfigure BFD on the interface, and then reconfigure it. Then, the session will come up.

- CSCto07919

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

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

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

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

- 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.

- CSCto11025

  Symptoms: When traffic streams are classified into multiple classes included with LLQ on the tunnel interface and the crypto map applied to an interface, packets are dropped on crypto engine with buffers unavailable.

  Conditions: This symptom occurs when configuring GRE over IPSec with a crypto map on the main interface. This issue is seen when the QoS policy is configured, and there is congestion.

  Workaround: Use tunnel protection or VTI instead of the crypto map on the interface.

- CSCto13254

  Symptoms: Anyconnect fails to connect to a Cisco IOS headend. The Anyconnect event log shows the following error:

  ```
  Hash verification failed for file <temp location of profile>
  ```

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

  Workaround: Remove the profile from the Cisco IOS headend.

- CSCto13338

  Symptoms: When a PSTN phone is calling an IP phone that is forwarded to a PSTN destination, the call is placed but no audio is present. This is the same behavior with blind transfer to external destinations.

  Conditions: This symptom occurs when voice-class codec X offer all and transcoders are used with CUBE.

  Workaround 1: Use the **codec XXXX** command instead of voice-class codec X offer all.

  Workaround 2: Use consultative transfer instead of blind transfer.

- CSCto15361

  Symptoms: MF: Active Supervisor crashes after removing the “router eigrp” configuration.

Conditions: This symptom occurs when the Active Supervisor crashes while disabling the IPv6 router EIGRP because the EIGRP Hello process gets killed. This issue occurs because the EIGRP Hello process calculates the size of the packet. After investigation, it was found that this is purely a timing-based issue. During cleanup, which is done by the EIGRP PDM process, the peer list is cleaned up first, and then an attempt is made to kill the Hello process. In case the peer list is cleaned up, and then the Hello process tries to calculate the size of a particular peer, then it finds the peer as NULL and crashes.

Workaround: Modify the igrp2_procinfo_free function to kill the EIGRP Hello process prior to cleaning up the peer list.

- CSCto16597

  Symptoms: When using the voluntary PPP feature with L2TP, a memory leak is seen. The leak is of AAA memory that is allocated on behalf of the voluntary PPP.

  Conditions: This symptom occurs when there is a disconnect of the L2TP or voluntary PPP connection.

  Workaround: There is no workaround.

- CSCto23807

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

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

  Workaround: There is no workaround.

- CSCto24338

  Symptoms: Router reload occurs due to the following bus error when the processor reads data from an invalid memory location:

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

  Conditions: This symptom occurs with NAT+SIP.

  Workaround: Disable the NAT SIP multipart processing by executing the **no ip nat service allow-multipart** command.

- CSCto31265

  Symptoms: ABR does not translate Type7 when primary Type7 is deleted even if another Type7 LSA is available.

  Conditions: This symptom occurs with OSPFv3. ABR receives multiple Type7 LSA for the same prefix from Multiple ASBR.

  Workaround 1: Delete/readd the static route that generates Type7.

  Workaround 2: Execute the **clear ipv6 ospf force-spf** command on ABR.

  Workaround 3: Execute the **clear ipv6 ospf redistribution** command on ASBR.

- CSCto34844

  Symptoms: The Cisco 891 may perform lower than the older generation Cisco 1812 platform.

  Conditions: This symptom occurs when Ethernet traffic using the VLAN tag is encapsulated inside the L2TPv3 tunnel.

  Workaround: There is no workaround.

- CSCto41165

  Symptoms: The standby router reloads when you use the **ip extcommunity-list 55 permit|deny** command, and then the **no ip extcommunity-list 55 permit|deny** command.

  Conditions: This symptom occurs when the standby router is configured.

  Workaround: There is no workaround.

- CSCto41173

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

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

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

- CSCto44581

  Symptoms: The router crashes on high call volume.

  Conditions: This symptom occurs on high call volume.

  Workaround: There is no workaround.

- CSCto46716

  Symptoms: Routes over the MPLS TE tunnel are not present in the routing table.

  Conditions: This symptom occurs when the MPLS TE tunnel is configured with forwarding adjacency. In “debug ip ospf spf”, when the SPF process link for the TE tunnel is in its own RTR LSA, the “Add path fails: no output interface” message is displayed. Note that not all tunnels are affected. It is unpredictable which tunnel is affected, but the number of affected tunnels grows with the number of configured tunnels.

  Workaround: If feasible, use autoroute announce instead of forwarding adjacency. Otherwise, upgrade to the fixed version.

- CSCto47524

  Symptoms: A Cisco ASR 1002 router that is running Cisco IOS Release 15.1(1)S1 may have a processor pool memory leak in IP SLAs Responder.

  A **show process memory sorted** command may initially show “MallocLite” growing. By disabling malloclite with the following:

  ```
  config t
  no memory lite
  end
  ```

  One may start to see the process “IP SLAs Responder” growing. In at least one specific case, the leak rate was 80MB per day.

  Conditions: This symptom is observed on a Cisco ASR 1002 router.

  Workaround: Disable IP SLA on the affected router, if possible.

- CSCto50255

  Symptoms: Memory leak occurs while running the UDP echo operation.

  Conditions: This symptom is observed when a UDP echo operation successfully runs. The leak is seen on every 100th run of the UDP echo operation. Using the **show memory debug leaks** command will not capture this. The only way is monitoring and decoding the PC via the **show processes memory** *pid* command.

  Workaround: There is no workaround.

- CSCto53332

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

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

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

  Conditions: This symptom occurs when IPSec accounting is active.

  Workaround: There is no workaround.

- CSCto63417

  Symptoms: A spurious access or crash occurs after applying the service policy.

  Conditions: This symptom occurs specifically when applying service-policy type access-control. This issue occurs when a large amount of traffic is being sent to the interface. The class-map uses RegEx in the match statement.

  For example:

  ```
    class-map type access-control match-any bittorrent
      match start l2-start offset 54 size 32 regex "GETinfo_hash="
      match start l2-start offset 54 size 32 regex
  "[a|A][z|Z][v|V][e|E][r|R]
  ```

  Workaround: Apply the service policy during low traffic or do not use RegEx in match statements.

- CSCto63954

  Symptoms: A router with GETVPN configurations is continuously crashing.

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

  Workaround: There is no workaround.

- CSCto68554

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

  These vulnerabilities are:

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

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are not available.

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

- CSCto71744

  Symptoms: FXO interfaces with the cable-detect feature enabled will automatically transition to the off-hook state when no PSTN battery voltage is detected, and remain off-hook for a duration of up to 1 minute. This condition violates regulatory telecom standards in several countries, including but not limited to the USA and Canada.

  The failing clauses of regulatory standards are as follows:

  - TIA-968-B 5.1.11.3
  - TIA-968-B 5.1.12.3
  - Industry Canada CS-03 Part I, Issue 9 December 2010

Conditions: This symptom occurs when the FXO interface is up, and the cable is connected to PSTN. Any interruption of the PSTN battery to FXO induces the off-hook condition, and the port does not transition back to on-hook for up to 1 minute.

Workaround: Disable the cable-detect feature in the FXO <config-voiceport> prompt. You can enable the feature in topologies that are not subject to regulatory standards (that is, on-premise installations).

- CSCto81814

  Symptoms: When SSH is attempted over an IKEv2 tunnel using ECDSA certificates, the router crashes.

  Conditions: This symptom is observed only when ECDSA certificates are used for IKEv2 and not with RSA certificates or with IKEv1.

  Workaround: There is no workaround.

- CSCto88686

  Symptoms: UCM cores when receiving SIPPublishReq with port “0”.

  SDI trace:

  ```
  13:15:18.735 |//SIP/Stack/Transport/0xd1e9460/msg=0xb7cee278, addr=xxx.xxx.xxx.xxx,
  port=0
  ```

  Conditions: This symptom occurs with the following conditions:

  – Configure the SIP trunk destination address as an IP address. The destination address is an SRV checkbox that is not checked.

  – Destination port = 0.

  Workaround: Modify the SIP trunk configuration to utilize a port in the defined valid port range between 1024 and 65535.

- CSCto99523

  Symptoms: Convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR).

  Conditions: This symptom occurs when convergence can take more time if there are a lot of VRF/routes and aggregation is configured in many VRFs. Massive route churn happens (for example, session reset with RR). There is no functionality impact.

  Workaround: There is no workaround.

- CSCtq04117

  Symptoms: DUT and RTRA have IBGP-VPNv4 connection that is established via loopback. OSPF provides reachability to BGP next hop, and BFD is running.

  Conditions: This symptom occurs under the following conditions:

  1. DUT has learned VPNv4 route from RTRA, and the same RD import is done at DUT.
  2. When switchover is performed in RTRA and when GR processing is done, the route is never imported to VRF.

  Workaround: Use the **clear ip route vrf x *** command.

- CSCtq05004

  Symptoms: Dialer loses the IP address sporadically. Shut/no shut on the ATM interface does not help.

  Conditions: There are no conditions so far. The behaviour is sporadic.

Workaround: Reload.

- CSCtq05636

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

  For example:

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

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

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

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

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

- CSCtq06538

  Symptoms: The RP crashes due to bad chunk in MallocLite.

  Conditions: This symptom occurs while executing testcase number 4883. The test case 4883 sends an incorrect BGP update to the router to test whether the router is able to handle the problematic update. The incorrect BGP update has the local preference attribute length incorrect:

```
LOCAL_PREF
  Header
    AttributeFlags
      Optional: 0b0
      Transitive: 0b1
      Partial: 0b0
      ExtendedLength: 0b0
      Unused: 0b0 0b0 0b0 0b0
    TypeCode: 0x05
    Length: 0x01     <----- should be 0x04 instead
  Value: 0xff 0xff 0xff 0xff
NetworkLayerReachabilityInfo: 0x08 0x0a <snip>
```

  Workaround: There is no workaround.

- CSCtq09899

  Symptoms: The VXML gateway crashes.

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

  Workaround: There is no workaround.

- CSCtq10684

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

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

  Workaround: A possible workaround is to reload the box.

- CSCtq15247

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

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

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

For example:

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

- CSCtq27180

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

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

  Workaround: There is no workaround.

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

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

- CSCtq28151

  Symptoms: A bus error crash occurs.

  Conditions: This symptom is observed on a Cisco 3900 voice gateway running Cisco IOS Release 15.1(3)T1.

  Workaround: There is no workaround.

- CSCtq28732

  Symptoms: Memory leak is observed when device is configured **parameter-map type inspectglobal**.

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

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

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

  Workaround: There is no workaround.

- CSCtq29554

  Symptoms: All multicast routes may be missing from the multicast forwarding information base (MFIB) after SSO and MFIB/MRIB error messages may be generated, indicating failure to connect MFIB tables to the MRIB. The output of the **show ipc port | in MRIB** command on a failed line card does not display a port.

Conditions: This symptom can occur on a line card of a distributed router such as the Cisco 7600 if an IPC local error has occurred before switchover. The MRIB IPC port to the new RP is not created after switchover and the MFIB tables cannot connect to the MRIB and download multicast routes.

Workaround: Reload the failing line card to recover it.

- CSCtq30875

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

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

  Workaround: The clock can be set manually via CLI.

- CSCtq39406

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

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

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

- CSCtq49408

  Symptoms: Analog phone calls (fxs) cannot be made with CME/SCCP.

  Conditions: This symptom occurs when SCCP support for FXS is missing in IAD2435.

  Workaround: There is no workaround.

- CSCtq61850

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

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

  Workaround: There is no workaround.

- CSCtq62322

  Symptoms: On an SNR call, when the call is forward and connected to CUE after ringing to the remote target, nothing happens (for example, no CUE prompt occurs, and the user cannot leave voice mail).

  Conditions: This symptom is observed if the answer-too-soon timer is configured, the remote target is a pstn call, and the calling party is using a sccp phone.

  Workaround: There is no workaround.

- CSCtq62759

  Symptoms: The CLNS routing table is not updated when the LAN interface with CLNS router ISIS configured shuts down because ISIS LSP is not regenerated. The CLNS route will be cleared after 10 minutes when ISIS ages out the stale routes.

  Conditions: This symptom is seen when only the CLNS router ISIS is enabled on the LAN interface. If IPv4/IPv6 ISIS is enabled, ISIS LSP will be updated.

  Workaround: Use the **clear clns route** command or the **clear isis *** command.

- CSCtq64951

  Symptoms: The following message is displayed:

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

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

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

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

  ```
  WebVPN context name: SSL_Context

  Client_Login_Name Client_IP_Address No_of_Connections Created Last_Used
  ```

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

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

- CSCtq77274

  Symptoms: FXS phones are not recognized as SCCP endpoints.

  Conditions: This symptom occurs when FXS phones are configured as SCCP endpoints.

  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.

- CSCtq86515

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

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

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

- CSCtq91176

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

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

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

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

- CSCtq92182

  Symptoms: An eBGP session is not established.

  Conditions: This issue is observed when IPv6 mapped IPv4 addresses are used, such as ::10.10.10.1.

  Workaround: Use an IPv6 neighbor address with bits. Set some higher bits along with the IPv4 mapped address.

- CSCtr26373

  Symptoms: The interface bounces, and after coming back up, hangs and does not pass traffic. The Rx ring is stuck and it may be observed that all packets coming into the interface are counted as “input errors”.

  Conditions: This symptom has been observed on the Cisco 3900. This issue may be seen at random times and has thus far been observed to happen after an interface bounce. The interface will still show “up/up” in the **show interface** command output.

  Workaround: Bounce the interface again to restore service.

- CSCti72131

  Symptoms: An additional static route is seen in the routing table.

  Conditions: This symptom occurs when you configure a static route with the DHCP option.

  Workaround: There is no workaround.

- CSCtr50118

  Symptoms: The router crashes.

  Conditions: This symptom occurs when the presence feature is turned on.

  Workaround: There is no workaround.

- 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.

Resolved Caveats—Cisco IOS Release 15.1(3)T1

Cisco IOS Release 15.1(3)T1 is a rebuild release for Cisco IOS Release 15.1(3)T. The caveats in this section are resolved in Cisco IOS Release 15.1(3)T1 but may be open in previous Cisco IOS releases.

- CSCtd91542

  Symptoms: The **show ip multicast rpf tracked** command may cause a crash.

  Conditions: This symptom is observed on a Cisco 10000 series router that is running all Cisco IOS 12.2(33) releases and after executing the **show ip multicast rpf tracked** command.

  Workaround: Avoid using the **show ip multicast rpf tracked** command.

Further Problem Description: The **show ip multicast rpf tracked** command is not intended for customer use and is being deprecated.

- CSCtf36402

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

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

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

- CSCtf54561

  Symptoms: A MPLS TE FRR-enabled router can encounter a crash if the **show ip cef vrf** *vrf-name* command is issued.

  Conditions: This symptom occurs when the VRF contains many entries (17k) in which the outgoing interface changes due to a topology change.

  Workaround: The command should not be issued when many topology changes occur on interface flaps.

- 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: This symptom is observed when an unknown notify message is received.

  Workaround: There is no workaround.

- CSCtf71673

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

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

  Workaround: There is no workaround.

- CSCtf72328

  Symptoms: BFD IPv4 Static does not fully support AdminDown.

  Conditions: This symptom is observed with the following setup and configuration:

  Router 1:

```
interface e0/0
ip address 192.168.1.1 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.10.1.1 255.255.0.0
exit
ip route static bfd e0/0 192.168.1.2
ip route 10.20.0.0 255.255.0.0 e0/0 192.168.1.2
```

  Router 2:

```
interface e0/0
ip address 192.168.1.2 255.255.255.0
bfd interval 51 min_rx 51 multiplier 4
bfd echo
no shut
exit

interface loopback 0
ip address 10.20.1.1 255.255.0.0
exit
ip route static bfd e0/0 192.168.1.1
ip route 10.10.0.0 255.255.0.0 e0/0 192.168.1.1

interface e0/0
no ip route static bfd e0/0 192.168.1.1
```

Though the BFD state is DOWN, the static has the route active. If the BFD peer signals AdminDown on a session being used to monitor the gateway for a static route, no action will be taken.

Workaround: Perform a shut/no shut the interface on which the BFD session is configured.

- CSCtg64175

  Symptoms: The ISIS route is missing the P2P link; it is mistakenly marked as “parallel p2p adjacency suppressed”.

  Conditions: This symptom is observed when the ISIS neighbor is up and multiple topologies are enabled on P2P interfaces. It is seen if you enable a topology on a P2P interface of the remote router and send out the serial IIH packet with the new MTID to the local router where the topology has not been enabled on the local P2P interface yet.

  Workaround: Do a shut and no shut on the local P2P interface.

- CSCtg72481

  Symptoms: Spurious memory access is seen with QoS configurations.

  Conditions: This symptom is observed only when sending the traffic for a while.

  Workaround: There is no workaround.

- CSCtg73631

  Symptoms: Spurious access or crash.

  Conditions: EIGRP undergoes a route delete event for a route that is both redistributed and learned as an external. The redistributed route is deleted and external route promoted. An error in the route deletion codepath may result in spurious access or crash.

  Workaround: There is no workaround.

  Further Problem Description: This issue is not present in Cisco IOS Release 15.0(1)M4.

- CSCtg91572

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

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

  Workaround: There is no workaround.

- CSCth20696

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

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

  Workaround: There is no workaround.

- CSCth37580

  Symptoms: Dampening route is present even after removing “bgp dampening”.

  Conditions: This symptom is observed under the following conditions:

  - DUT connects to RTRA with eBGP + VPNv4.
  - eBGP + VPNv4 peer session is established and DUT.
  - Also, DUT has VRF (same RD) as the route advertised by RTRA.

  In this scenario, when DUT learns the route, it will do the same RD import and the net’s topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

  Workaround: There is no workaround.

- CSCth84233

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

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

  Workaround: Remove “qos pre-classify”.

- CSCth93218

  Symptoms: The error message “%OER_BR-4-WARNING: No sequence available” is displayed on PfR BR.

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

  Workaround: There is no workaround.

- CSCti22091

  Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually re-enabling PfR will not work. A reboot is required.

  Conditions: This symptom is observed when PfR is configured with the following conditions:

  1. list > application > filter > prefix-list
  2. Learn > traffic-class: keys
  3. Learn > traffic-class: filter > ACL

  Workaround: There is no workaround.

- 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

- CSCti34396

  Symptoms: The router distributes an unreachable next hop for a VPNv4 or VPNv6 address as an MVPN tunnel endpoint.

  Conditions: This symptom is observed when "next-hop-unchanged allpaths" is configured for an external neighbor of the VPNv4 or VPNv6 tunnel endpoint, and the previous hop is unreachable.

  Workaround 1: Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside of it. For example, to rewrite statically configured routes so that the next hop is set to a visible address, you would configure:

```
route-map static-nexthop-rewrite permit 10
match source-protocol static
    set ip next-hop <router ip address>
!
router bgp <asn>
    address-family ipv4 vrf <vrf name>
    redistribute static route-map static-nexthop-rewrite
    exit-address-family
    exit
exit
```

  Workaround 2: Instead of configuring static routes with a next hop, specify an interface name.

  For example, if you had:

```
ip route x.x.x.x 255.255.255.0 y.y.y.y
```

  And y.y.y.y was on the other end of the interface serial2/0, you would replace this configuration with:

```
ip route x.x.x.x 255.255.255.0 interface serial2/0
```

  Further Problem Description: You may also need to override the standard behavior of next-hop-unchanged allpaths in a generic manner with a single standard configuration which could be applied to all the routers. In order to solve this problem, the configuration "set ip next-hop self" is added to route-maps.

  When used in conjunction with the newly added configuration:

```
router bgp <asn>
    address-family vpnv4 unicast
      bgp route-map priority
```

  The "set ip next-hop self" will override "next-hop unchanged allpaths" for the routes which match the route-map where it is configured, allowing the selective setting of the next-hop.

- CSCti50607

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

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

Workaround: There is no workaround.

- CSCti51145

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

  Conditions: In order to see this problem, ALL of the following conditions must be met:

  - The nonreloading device must have a "neighbor x.x.x.x transport connection-mode passive" configuration, or there must be an ip access list or packet filter that permits connections initiated by the reloading device, but not by the nonreloading device. In Cisco IOS, such ip access-lists typically use the keyword **established** or **eq bgp**.
  - It must be configured with a BGP hold time which is less than the time required for the neighbor x.x.x.x to reload.
  - When the neighbor x.x.x.x reloads, no keepalives or updates must be sent on the stale session during the interval between when the interface comes up and when the neighbor x.x.x.x exchanges BGP open messages.
  - Both peers must be multisession capable.
  - "transport multi-session" must not be configured on either device, or enabled by default on either device.
  - "graceful restart" must not be configured.

  Workarounds:

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

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

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

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

- CSCti61949

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

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

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

- CSCti66076

  Symptoms: A standby HSRP router could be unknown after reloading the ES20 module that configured HSRP.

  Condition: This symptom is observed under the following conditions:

  - HSRP version 1 is the protocol that must be used.
  - Use HSRP with sub-interfaces on ES20 module.
  - Reload the ES20 module.

  Workaround: Change to HSRPv2, which is not exposed to the issue.

  Alternate Workarounds:

  1. Reconfigure HSRP on all subinterfaces.
  2. Configure multicast or igmp configuration on the interface where HSRP is configured (like ip pim sparse-mode).

- CSCti67102

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

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

  Workaround: There is no workaround.

- CSCti67905

  Symptoms: A Cisco router may experience a crash.

  Conditions: This has been experienced on Cisco routers running Cisco IOS Release 15.1(2)T and Cisco IOS Release 15.1(2)T1. The routers are configured with IOS firewall and are inspecting FTP packets.

  Workaround: There is no workaround.

- CSCti68721

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

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

  Workaround: If the symptom occurs, repeat the command.

- CSCti75666

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

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

  Workaround: Convert H.323 leg to SIP.

- CSCti79848

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

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

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are not available.

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

- CSCti84762

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

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

  Workaround: Do a hard reset of the stuck peers.

- CSCti85446

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

  Conditions: This symptom is observed with the following conditions:

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

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

- CSCti87502

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

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

  Workaround: A power cycle fixes the issue temporarily.

- CSCti88897

  Symptoms: When configuring the interface cellular 0 on a Cisco 880 series router that is running Cisco IOS Release 15.1(1)T1 or up to Cisco IOS Release 15.1(2) T1, the **service-policy output QOS_CUST_BASIC_OUT** command disappears when the router is reloaded or power cycled.

  Conditions: This symptom is observed with Cisco IOS Release 15.1(1)T1 or up to Cisco IOS Release 15.1(2)T1.

  Workaround: There is no workaround.

- CSCti91036

  Symptoms: Performance drop has been seen between Cisco IOS Release 15.1(1)T and Cisco IOS Release 15.1(2)T.

  Conditions: This symptom is observed when you upgrade from Cisco IOS Release 15.1(1)T to Cisco IOS Release 15.1(2)T.

- 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.

  Workaround: There is no workaround.

- CSCtj00039

  Symptoms: Some prefixes are in the PE router EIGRP topology although those routes are not being passed to the CE router.

  Conditions: This symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

  Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj05198

  Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

  Conditions: This symptom is observed when there are two EIGRP router processes.

  Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj07885

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

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

  Workaround:

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

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

     -Turn off SNMP polling on the device.

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

- CSCtj07904

  Symptoms: EIGRP neighbor relationship goes down with “no passive interface” configured.

  Conditions: This symptom is observed when “no passive interface” is configured.

Workaround: Do not configure “passive-interface default” and allow the interface to be nonpassive by default. Configure “passive-interface <interface>” for the interface to be passive.

- CSCtj08533

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

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

  Workaround: Use only one path between PE and CPE.

- CSCtj15798

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

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

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

- CSCtj17545

  Symptoms: Immediately after a switchover, the restarting speaker sends TCP-FIN to the receiving speaker, when the receiving speaker tries to establish (Active open). It can cause packet drops after a switchover.

  Conditions: This symptom can occur when a lot of BGP peers are established on different interfaces.

  Workaround: When the receiving speaker is configured to accept passive connections, the issue will not be observed:

  ```
  template peer-session ce-v4
      transport connection-mode passive
  ```

- CSCtj20163

  Symptoms: On a PE1-P-PE3 setup, a crash is seen on P (core) router with scaled MLDP configurations.

  Conditions: This symptom is observed with the following conditions:

  1. Execute **show mpls mldp database**.
  2. Reload Encap PE.
  3. Crash seen on P router when MLDP neighbors go down.

  Workaround: There is no workaround.

- CSCtj21696

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

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

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

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

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

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

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

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

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

- CSCtj24453

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

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

  Conditions: It is rarely observed, when **clear ip bgp *** is done with lot of routes and route-map-cache entries.

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

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

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

- CSCtj27251

  Symptoms: A router may crash when modifying a QoS class-map.

  Conditions: This symptom is observed when modifying a QoS class-map which is being referenced by two or more policy-maps while traffic is matching the class-map and traversing the router.

  Workaround: Remove the policy-maps that match the class-map to be modified by issuing **no service-policy input/output** *policy-map name*, make changes to the class-map, and then re-apply the policy-maps by issuing **service-policy input/output** *policy-map name*.

- CSCtj28747

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

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

  Workaround: There is no workaround.

- CSCtj39558

  Symptoms: Subinterface queue depth cannot be configured.

Conditions: This symptom is observed when the policy is attached to ethernet subinterfaces.

Workaround: There is no workaround.

- CSCtj40564

  Symptoms: The Cisco ASR 1000 router disallows an incoming Internet Key Exchange (IKE) connection that matches a keyring. This issue occurs after the router is reloaded.

  Conditions: This symptom occurs when a crypto keyring, which has a local-address defined as an interface, is used.

```
crypto keyring keyring_test
    pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted>
    local address Loopback2104
```

  Workaround: Use an IP address.

```
crypto keyring keyring_test
    pre-shared-key address 0.0.0.0 0.0.0.0 key <omitted>
    local address <ip address>
```

- CSCtj41194

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

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

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

- CSCtj47736

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

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

  Workaround: There is no workaround.

- CSCtj48629

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

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

  Workaround: There is no workaround.

- CSCtj52077

  Symptoms: The policy at the subinterface is not accepted with CBWFQ.

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

  Workaround: There is no workaround.

- CSCtj58943

  Symptoms: The standby RP reloads due to line-by-line sync failure for the **encapsulation dot1q 1381** command:

```
Config Sync: Line-by-Line sync verifying failure on command:
    encap dot1Q 1381
due to parser return error
```

```
rf_reload_peer_stub: RP sending reload request to Standby. User: Config-Sync,
Reason: Configuration mismatch
```

Conditions: This symptom occurs when issuing a configuration command under a subinterface mode.

Workaround: There is no workaround.

- CSCtj65553

  Symptoms: The static route that is installed in default table is missing.

  Conditions: The static route is missing after Route Processor (RC) to Line Card (LP) to Route Processor transition on the Cisco Catalyst 3000 series switching module.

  Workaround: Configure the missing static route.

- CSCtj66235

  Symptoms: A UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to software-forced crash while experiencing the following error:

  ```
  %SYS-6-STACKLOW: Stack for process voice
  file acct dump running low, 0/6000
  ```

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

  Workaround: There is no workaround.

- CSCtj67845

  Symptoms: A Cisco 2951 router crashes on power up.

  Conditions: This symptom is observed on a Cisco 2951 router when an HWIC-ADSL and EHWIC-VA-DSL are plugged in together.

  Workaround: There is no workaround.

- CSCtj68636

  Symptoms: WAAS_Express trial license is missing in Cisco IOS universalk9_npe image for Cisco 880 and 890 platforms.

  Conditions: This symptom occurs while using the WAAS Express trial license.

  Workaround: Install the Cisco IOS WAAS Express permanent license.

- CSCtj69886

  Symptoms: NTP multicast over multiple hops.

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

  Workaround: There is no workaround.

- CSCtj77004

  Symptoms: Archive log configuration size impacts CPU utilization during PPPoE establishment. Also, only some configuration lines from the virtual-template are copied to archive (some lines missing).

  Conditions: The symptom is observed when “archive log config” is configured.

  Workaround: There is no workaround.

- CSCtj77477

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

For example: EFM rate 2304 kbps

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

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

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

For example: EFM rate 2304 kbps

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

- CSCtj77963

  Symptoms: Resets are observed on low-speed links.

  Conditions: This symptom is observed on low-speed interfaces over the WAN that produce retransmissions, out of order segments, etc.

  Workaround: There is no workaround.

- CSCtj78210

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

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

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

  For example, perform the following configurations:

```
voice-card 0 (1... 2... etc...)
dspfarm
dsp service dspfarm

dspfarm profile x conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown

dspfarm profile x2 conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown

dspfarm profile x3 conf
max sessions xx << use maximum (if allowed)
max partic << use the maximum (if allowed)
```

```
associate app sccp
no shutdown

dspfarm profile x conf
shutdown
no dspfarm profile x conf
```

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

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

- CSCtj81533

  Symptoms: The following error message is seen:

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

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

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

  Workaround: There is no workaround.

- CSCtj82292

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

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

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

  Workaround: There is no workaround.

- CSCtj84901

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

  Conditions: This symptom is observed on Cisco 1900 series, 2911, and 2921 routers with PVDM modules, as well as any other module that connects to the MGF backplane switch. The following modules currently connect to MGF:

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

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

  This symptom is not observed on Cisco 2951, 3900 series, or 3900e series routers.

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

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

- CSCtj85333

  Symptoms: System may crash when config-template contains the config command **ip ips signature-category** and when the template is downloaded to the router using the CNS configuration feature using the **cns config retrieve** EXEC command and the **cns config initial** configuration command. This symptom may also occur when the configuration template is downloaded to the router using the device config-update operation of the configuration engine.

  Conditions: This is normal mode operation, but this symptom will occur when any such CNS features are used.

  Workaround: There is no workaround.

- CSCtj87180

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

  Conditions: 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 multi-hop peer.

  Workaround: There is no workaround.

- CSCtj89941

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

  Conditions: This symptom is observed with the following test bed setup:

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

  Workaround: There is no workaround.

- CSCtj90438

  Symptoms: Router crashes if “no switchport” is executed on /1 interface of Enhanced EtherSwitch (ESW) or Service Ready Engine (SRE) module.

  Conditions: This symptom occurs while executing “no switchport” on the /1 interface of ESW or SRE module without HWIC-4ESW, HWIC-D-9ESW, HWIC-4ESW-POE, HWIC-D-9ESW-POE, NM-16ESW, and NM-16ESW-1GIG present.

  Workaround: Do not execute the **no switchport** command on the above mentioned modules as this command does not apply to these modules.

- CSCtj91764

  Symptoms: A Cisco UC560 or UC540 platform that is running Cisco IOS Release 15.1(2)T1 reloads due to an unexpected exception to the CPU.

  Conditions: This symptom occurs during a complete SNMP MIB walk.

  Workaround: Exclude the CISCO-CALL-APPLICATION-MIB via configuration.

- CSCtj94297

  Symptoms: “F” flag gets set in the extranet receiver MFIB forwarding entry, resulting in unexpected platform behavior.

Conditions: The symptom is observed when the forwarding entry RPF transitions from a NULL/local interface to an interface belonging to a different MVRF.

Workaround: Use the **clear ip mroute** command in the affected mroute.

- CSCtk02647

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

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

  Workaround: There is no workaround.

- CSCtk06548

  Symptoms: Using CCBU CVP solution, SIP calls are disconnected during stress test.

  Conditions: This symptom is observed when using a TCP connection. SIP messages are sporadically corrupted and cannot be framed correctly by SIP stack. It is seen with PI14 image testing.

  Workaround: Use PI12 image.

  Further Problem Description: The fundamental issue involves the selective ack (SACK) feature. An alternative workaround would be to disable the “SACK Permitted” option from the peer.

- CSCtk12608

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

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

```
Router 1:
interface Ethernet0/0
  ip address 10.0.12.1 255.255.255.0
!
interface Ethernet1/0
  ip address 10.0.120.1 255.255.255.0
!
router bgp 100
  no synchronization
  bgp log-neighbor-changes
  neighbor 172.16.0.1 remote-as 200
  neighbor 172.16.0.1 ebgp-multihop 255
  no auto-summary
!

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

Router 2:
 interface Loopback200
 ip address 10.10.200.1 255.255.255.0
!
interface Loopback201
  ip address 172.16.0.1 255.255.255.0
!
interface Ethernet0/0
  ip address 10.0.12.2 255.255.255.0
!
interface Ethernet1/0
  ip address 10.0.120.2 255.255.255.0
```

```
!
router bgp 200
 no synchronization
 bgp log-neighbor-changes
 network 10.10.200.0
 neighbor 10.0.12.1 remote-as 100
 neighbor 10.0.12.1 update-source Loopback201
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.0.12.1
!
```

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

- CSCtk35953

  Symptoms: The dampening information will not be removed even if dampening is unconfigured in VPNv4 AF.

  Conditions: The symptom is observed only if DUT has eBGP-VPNv4 session with a peer and a same-RD is imported on the DUT for the route learned from VPNv4 peer.

  Workaround: A hard reset of the session removes the dampening information.

- CSCtk46363

  Symptom: A device running Cisco IOS and acting as a DHCP server crashes.

  Conditions: This symptom is observed when a client requests a specific IP address.

  Workaround: Disable duplicate address detection check using the **ip dhcp ping packet 0** command.

- CSCtk47891

  Symptoms: If Fast Reroute (FRR) is in use, the traffic might be blackholed when LC is reset.

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

  Workaround: There is no workaround.

- CSCtk52599

  Symptoms: A Cisco 888E router does not train up with a third-party vendor's DSLAM.

  Conditions: The symptom is observed when the DSLAM is running new firmware.

  Workaround: There is no workaround.

- CSCtk53130

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

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

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

  Workaround: There is no workaround.

- CSCtk53534

  Symptoms: Router crashes.

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

  Workaround: Disable global parameter-map.

- CSCtk56570

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

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

  Workaround: Disable media transcoder-high-density.

- CSCtk56817

  Symptoms: Router crashes.

  Conditions: The symptom is observed when pinging the dialer interface attached to the ATM interface.

  Workaround: There is no workaround.

- CSCtk58732

  Symptoms: The router may crash if the following configuration is applied:

```
ip sla 1
icmp-jitter 192.0.2.1 source-ip 192.0.2.2 num-packets 1 interval 10
threshold 1000
timeout 1000
frequency 10
ip sla schedule 1 start-time now life forever
track 1 ip sla 1 reachability
```

  The following error message is displayed:

```
%ALIGN-1-FATAL: Illegal access to a low address 10:49:31 UTC Mon Feb 21 2011 addr=0x1,
pc=0x62D97F30z , ra=0x62D98848z , sp=0x67CE34D0
10:49:31 UTC Mon Feb 21 2011: Address Error (store) exception, CPU signal 10, PC =
0x62DA2E10
```

  Conditions: This symptom occurs in Cisco IOS Release 15.1(3)T release. The router may continually reload following the crash.

  Workaround: Use the ICMP Echo operation instead, as shown below:

```
ip sla 1
icmp-echo 192.0.2.1 source-ip 192.0.2.2
threshold 1000
timeout 1000
frequency 10
```

- CSCtk61069

  Symptoms: The Cisco IOS router crashes.

  Conditions: This symptom occurs while using the **write memory** or **show running configuration** commands on the router, after configuring “privilege exec level 15 show adjacency”.

  Workaround: Do not set the privilege EXEC level for any form of the **show adjacency** command.

- CSCtk62247

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

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

  Workaround: Use non-hierarchical CA servers.

- CSCtk67709

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

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

Conditions: This symptom is observed with AnyConnect 3.0.

Workaround: There is no workaround.

- CSCtk74970

  Symptoms: TE autoroute-announced tunnel is not installed in the routing table.

  Conditions: The symptom is observed if you configure TE with one hop-LDP and then unconfigure. Then configure TE with one hop with non-LDP. The TE autoroute-announced tunnel is not installed in the routing table.

  Workaround: Configure **no ip routing protocol purge interface**.

- CSCtk84116

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

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

  Workaround: There is no workaround.

- CSCtk95992

  Symptoms: DLSw circuits 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 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, and later releases.

- CSCtk96229

  Symptoms: Traceback occurs during reloading of the Cisco EtherSwitch module. Looping TCP packets are generated for the active session that exists between the router and switch module in the same router.

  Conditions: This symptom is observed when the Cisco EtherSwitch module reloads after you enter the switch module using the **service-module** *interface* command from the router.

  Workaround: There is no workaround.

- CSCtl02057

  Symptoms: Router crashes for ATM traffic with multiple GG cards.

  Conditions: This symptom occurs when both ATM and PTM modes are present in the router.

  Workaround: There is no workaround.

- CSCtl04285

  Symptoms: After a BGP flap or while provisioning a new session, the BGP route reflector will not advertise new IPv4 MDT routes to PEs.

  Conditions: This symptom is observed with BGP session flap or while provisioning a new session.

  Workaround: Enter the **clear ip bgp *** command.

- CSCtl05941

  Symptoms: CUBE crashes.

  Conditions: This symptom is observed when voice HA is configured on CUBE.

Workaround: There is no workaround.

- CSCtl08014

  Symptoms: Router crashes with memory corruption symptoms.

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

  Workaround: There is no workaround.

- CSCtl08594

  Symptoms: After upgrading to Cisco IOS Release 15.1(3)T, routers are not able to connect to the EZVPN server anymore. ISAKMP fails to find the key.

  Conditions: This symptom occurs with the following conditions:

  – DHCP is configured on outside interface.

  – Outside interface is FastEthernet.

  This symptom does not occur if the outside interface is VLAN. This symptom is not seen in Cisco IOS Release 15.1(2)T1.

  Workaround: Downgrade to 15.1(2)T1, use VLAN interface, or remove “ip route 0.0.0.0 0.0.0.0 fastethernet4 dhcp” statement from the config and 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 the LNS is configured for PPTP aggregation and over one millions tunnels have been accepted on VPDN level.

  Workaround: Reload LNS.

- CSCtl21884

  Symptoms: When enabling auto-summary under the BGP process, a BGP withdraw update is not sent, even though the static route goes down.

  Conditions: The symptom is observed under the following conditions:

  – Enable auto-summary under the BGP process.

  – Static route is brought into the BGP table via the **network** command.

  Workaround: Use the **clear ip bgp *** command or disable auto-summary under the BGP process.

- CSCtl44103

  Symptoms: The router crashes when Cisco 3945 router that is running Cisco IOS Release 15.1(3)T, has a zone-based firewall configured.

  Conditions: This symptom occurs when using any of the following three debug commands:

  – **debug policy-map type inspect events**

  – **debug policy-firewall events**

  – **debug ip inspect events**

  Workaround: There is no workaround.

- CSCtl47666

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

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

  Workaround: There is no workaround.

- CSCtl50815

  Symptoms: Prefixes remain uncontrolled. Additionally, the following message is logged frequently without any actual routing changes:

  ```
  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
  Non-OER, OOP Reason <reason>
  ```

  Conditions: The symptom is observed while using the following:

  - ECMP
  - **mode monitor passive**

  Workaround: Remove equal cost routing. For instance, if you currently use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one per exit. This achieves initial load balancing and PfR will balance the load correctly, as necessary.

  Further Problem Description: In some networks, when you are using equal cost load balancing, several flows that are mapped to a single traffic class/prefix in PfR might exit on more than just a single exit. This can lead to PfR not being able to properly learn the current exit and can cause PfR to be unable to control this traffic.

- CSCtl57055

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

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

  Workaround 1: Configure NMS to stop polling the “rttMonStatsTotalsEntry” or create a view and block the MIB on the router.

  Workaround 2: The issue only affects Cisco IOS 15.1T releases, so use a Cisco IOS 15.0(1)M rebuild or earlier.

- CSCtl67195

  Symptoms: The following three BGP debug commands cannot be enabled:

  - **debug ip bgp vpnv4 unicast**
  - **debug ip bgp vpnv6 unicast**
  - **debug ip bgp ipv6 unicast**

  Conditions: This symptom is observed with the above BGP debug commands.

  Workaround: There is no workaround.

- CSCtl71478

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

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

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

Workaround: There is no workaround.

- CSCtl73914

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

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

  Workaround: There is no workaround.

- CSCtl77735

  Symptoms: Saving a configuration to NVRAM may fail.

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

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

- 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.

- CSCtl88066

  Symptoms: A router reloads (seen with a Cisco ASR 1000 Series Aggregation Services router) or produces a spurious memory access (seen with most other platforms).

  Conditions: This symptom is observed when BGP is configured and you issue one of the following commands:

  – **show ip bgp all attr nexthop**

  – **show ip bgp all attr nexthop rib-filter**

  Workaround: Do not issue either of these commands with the "all" keyword. Instead, issue the address family-specific version of the command for the address family you are interested in.

  For example, the following are safe:

  – **show ip bgp ipv4 unicast attr nexthop**

  – **show ip bgp attr nexthop**

  – **show ip bgp vpnv4 vrf** *vrfname* **attr nexthop**

  Further Problem Description: While the **show ip bgp all attr nexthop** has never done anything that **show ip bgp attr nexthop** did not do, the reload bug was introduced during the development of multi-topology routing. All versions of Cisco IOS which include multi-topology routing or which are derived from versions which included multi-topology routing and where this fix is not integrated, are impacted.

  The fix prevents the issuing of commands beginning with **show ip bgp all attr**.

- CSCtl92014

  Symptoms: After a reprompt element, "enumerate", using internal variables like _prompt or _dmtf, no longer produces a valid list of options and repeats the last option.

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

Workaround: There is no workaround.

- CSCtl98270

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

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

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

- CSCtn01832

  Symptoms: The following command sequence crashes the router at check syntax mode:

  config check syntax

  route-map hello

  match local-preference

  no match local-preference

  Conditions: The symptom is observed with the above command sequence.

  Workaround: There is no workaround.

- CSCtn08613

  Symptoms: Cisco router crashes when interfacing with UCCX.

  Conditions: This has been experienced when making consult transfer calls on a Cisco UC560 platform that is running Cisco IOS Release 15.1(2)T2.

  Workaround: There is no workaround.

- CSCtn09135

  Symptoms: MC5728V modem is not enumerated resulting in cellular interface not coming up.

  Conditions: This symptom occurs more often with USB flash attached and on DSL SKUs.

  Workaround: Removing the USB flash solves the issue in some instances.

- CSCtn27599

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

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

  Workaround: There is no workaround.

- CSCtn51740

  Symptoms: Memory leak is seen in the EzVPN process.

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

  Workaround: There is no workaround.

- CSCtn63325

  Symptoms: The Cisco 1841 router crashes during firmware upgrade.

  Conditions: This symptom occurs when microcode CLI is used during firmware upgrade on the Cisco 1841 router.

  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.

Open Caveats—Cisco IOS Release 15.1(3)T

This section describes possibly unexpected behavior by Cisco IOS Release 15.1(3)T. All the caveats listed in this section are open in Cisco IOS Release 15.1(3)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsr89078

  Symptoms: A Cisco AS5400XM reloads unexpectedly on stress with high CPS voice calls and with H.323, g729r8, no VAD and limited DSPs.

  Conditions: The symptom is seen only when DSPs on a Cisco AS5400XM are less than the number of calls it can accommodate.

  Workaround: Have sufficient available DSPs.

- CSCsz05848

  Symptoms: High CPU utilization for DHCP client process.

  Conditions: The symptom is observed when 10k PDPs sessions are established.

  Workaround: There is no workaround.

- 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.

- CSCta40972

  Symptoms: The router produces the following message:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (8/4),process =
  BGP Router.
  ```
  followed by a traceback, and then both active and standby reload.

  Conditions: The symptom is observed when BGP is configured, and then “neighbor x.x.x.x ... prefix-list ...” is configured. This is known to happen at scale when many neighbors are configured, but the exact trigger conditions are not known.

  Workaround: Do not enter this CLI for a neighbor in an update-group with lots of other neighbors.

- CSCtb70595

  Symptoms: A Cisco router may experience a crash.

  Conditions: The symptom is observed on a Cisco 2851 router that is running Cisco IOS Release 12.4(25a).

  Workaround: There is no workaround.

- CSCtd42628

  Symptoms: Router reloads due to bus error following tunnel flaps.

  Conditions: The symptom is observed following tunnel flaps.

  Workaround: There is no workaround.

- CSCtd90030

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

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

  Workaround: There is no workaround.

- CSCtd91542

  Symptoms: The **show ip multicast rpf tracked** command may cause a crash.

  Conditions: The symptom is observed on a Cisco 10000 series router that is running all Cisco IOS 12.2(33) releases and after executing the **show ip multicast rpf tracked** command.

  Workaround: Avoid using the **show ip multicast rpf tracked** command.

  Further Problem Description: The command **show ip multicast rpf tracked** is not intended for customer use and is being deprecated.

- CSCte50870

  Symptoms: A Cisco AS5400 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 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.

- CSCte94221

  Symptoms: PPP connection over CDMA link is flapping.

  Conditions: The symptom is observed when using Cisco IOS Release 15.0M.

  Workaround: Shut / no shut the interface and wait for 2 mins.

- CSCtf72156

  Symptoms: When the ISDN phone makes a call to a PSTN phone which is switched off, no announcements are heard at the ISDN end.

  Conditions: The symptom is observed with a Cisco AS5400 but is independent of the IOS version on the router. There are no other specific conditions.

  Workaround: There is no workaround.

- CSCtg13009

  Symptoms: DSP crash due to heart beat error. Logs show the following output:

  ```
  %MSDSPRM-3-DSPCRASH: slot 3 dspId 3 heartBeat 022C9632 heartBeatError 1
  %MSDSPRM-3-DSPCRASH: slot 3 dspId 2 heartBeat 031FD34B heartBeatError
  1coil_show_controller
  ```
  The DSP reset causes no-way audio on conference adhoc or meet me bridge.

  Conditions: The symptom occurs during normal operations of ad-hoc and meet-me conferencing.

  Workaround: There is no workaround.

- CSCtg42271

  Symptoms: A router that is running Cisco IOS Release 15.0(1)M1 may experience a series of spurious memory access errors and a bus error when configured for IPS:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0xXXXXXXXX reading 0xXXX
  %ALIGN-3-TRACE: -Traceback= 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX 0xXXXXXXXX
  0xXXXXXXXX
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x70, pc=0x251A00CCz ,
  ra=0xFFFF3331z , sp=0x28F88EB0
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x70, pc=0x251A00CCz ,
  ra=0xFFFF3331z , sp=0x28F88EB0
  XX:XX:XX XXX XXX XXX XX XXXX: TLB (store) exception, CPU signal 10, PC = 0xXXXXXXXX
  ```
  Conditions: The symptom is observed when the device is configured for IPS and is running Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

- 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

- CSCtg67146

  Symptoms: File transfer to the flash fails with a “TF I/O failed in data-in phase” message. Archive command fails 100% of the time whereas a copy command is successful sometimes.

  Conditions: The symptom is observed when the router is running Cisco IOS Release 12.4(24)T or above and has a STI flash 7.2.0. The transfer fails with some delay (~50-100msec).

  Workarounds:

  1. Transfer without a delay.
  2. Transfer with Cisco IOS Release 12.4(9)T.
  3. Transfer with a newer flash card.

  Further Problem Description: Issue is seen with Cisco IOS Releases 12.4(24)T, 12.4(24)T1, 12.4(24)T2, 12.4(24)T3, and 15.1(1)T.

- 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.

- CSCtg68568

  Symptoms: A Cisco 3945 router configured as a GETVPN group member might crash when passing traffic.

  Conditions: The symptom occurs when fragmentation of the IP datagram is required due to MTU limit of 1500 bytes.

  Workaround: Configure hosts to negotiate lower TCP MSS (1360) bytes and avoid fragmentation.

- CSCtg72481

  Symptoms: Spurious memory access is seen with QoS configurations.

  Conditions: The symptom is observed only when sending the traffic for a while.

  Workaround: There is no workaround.

- CSCth14305

  Symptoms: Having a bandwidth statement on a multilink bundle interface will cause problems with QoS and BQS if linkmembers flap as the changes in bandwidth will not be handled correctly.

  Conditions: The symptom is observed when you have a bandwidth statement on a multilink bundle.

  Workaround: Avoid bandwidth statements on multilink bundle interfaces.

- CSCth19516

  Symptoms: A router crashes if you have PFR and SAF enabled on the same device.

  Conditions: The issue is seen when you have SAF enabled and PFR with multiple links. When the network gets congested or delay is seen and if there is a change over from IN-POLICY state to OOP the router crashes.

  Workaround: Disable SAF completely and reload the router.

- 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.

- CSCth23354

  Symptoms: Packets are not reaching the proper queue.

  Conditions: The symptom is observed when class-map is configured with VLAN.

  Workaround: There is no workaround.

- CSCth29426

  Symptoms: When you issue a **reload** command with a getmany looping on ciscoFlashMIB, the router hangs.

  Conditions: The symptom is observed when a getmany is running with only one router. The chances of hitting the issue seem to be increased if a **write memory** has been done before reload or even if the configuration is dirty and you respond "no" to the save configuration prompt.

  Workaround: Avoid reloading while doing an SNMP walk on ciscoFlashMIB.

- CSCth37580

  Symptoms: Dampening route is present even after removing "bgp dampening".

  Conditions: The symptom is observed under the following conditions:

  - DUT connects to RTRA with eBGP + VPNv4.
  - eBGP + VPNv4 peer session is established and DUT.
  - Also DUT has VRF (same RD) as route advertised by RTRA.

  In this scenario, when DUT learns the route it will do same RD import and the net's topology will be changed from VPNv4 to VRF. When dampening is unconfigured, we do not clear damp info.

  Workaround: There is no workaround.

- CSCth38565

  Symptoms: The router crashes after traffic stops and the WE router is unconfigured. This problem is intermittent and very difficult to reproduce.

  Conditions: The symptom is observed when the WE is configured for full optimization, traffic is passed and then the WE router is unconfigured. The type of traffic being passed does not seem to affect the crash.

  Workaround: There is no workaround.

- CSCth51168

  Symptoms: An H.323 to H.323 CUBE may incorrectly reuse existing TCP sockets when completing H.323 calls. This leads to call failures with cause values of:

  ```
  18 - No user responding
  ```
  or
  ```
  102 - Recovery on timer expiry
  ```
  Conditions: The symptom is observed on a Cisco 7206VXR CUBE handling 100+ calls with Cisco IOS Release 12.4(22)T5.

  Workaround: Disable reuse of TCP sockets with the following commands:

  voice service voip

  h323

  h225 timeout tcp call-idle value 0

session transport tcp calls-per-connection 1

- 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:

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

  This symptom has been seen with:

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

- CSCth64316

  Symptoms: Unable to configure “radius-server” using SNMP set.

  Conditions: The symptom is observed when you configure via SNMP MIB.

  Workaround: Radius server can be configured through the CLI.

- CSCth66604

  Symptoms: ISSU incompatibility due to different versions of a protocol (NTP v3 and NTP v4).

  Conditions: The symptom is observed with an ISSU upgrade or downgrade.

  Workaround: Unconfigure the CLIs causing MCL errors and repeat the ISSU process again.

- CSCth68038

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

- CSCth71648

  Symptoms: G3 fax fails.

  Conditions: The symptom is observed when T38 v3 is configured on gateway and Cisco fax server.

  Workaround: Configure gateway and fax server with T38 V0.

- CSCth77562

  Symptoms: Unable to read vlanTrunkPortEntry.13 object, but can set values to manage VLAN/Trunk mode configuration on NM-ESW16 ports.

  Conditions: The symptom is observed on a Cisco 2800 series router that is running Cisco IOS Release 12.4(24)T3.

  Workaround: There is no workaround.

- CSCth81055

  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.

  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-ike

  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

- CSCth84233

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

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

  Workaround: Remove "qos pre-classify".

- CSCth87041

  Symptoms: Router hangs.

  Conditions: The symptom is observed when unconfiguring "match field" under class map.

  Workaround: There is no workaround.

- CSCth87348

  Symptoms: Virtual access multilink interface fails to come up.

  Conditions: The symptom is observed when "frame-relay traffic-shaping" and O/P service policy are applied, then shut/no shut the interface.

  Workaround: There is no workaround.

- CSCth90147

  Symptoms: Router will respond to an RS with an RA.

  Conditions: The symptom is observed when you configure the command **ipv6 nd ra suppress**. This command is only intended to suppress periodic mcast RAs. The router will still respond to unicast RS (that is intended behavior).

  Workaround: Use an ACL to block the reception of RS packets.

- CSCth93218

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

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

  Workaround: There is no workaround.

- CSCti03199

  Symptoms: During switch-over, standby crashes after every recovery due to config-sync.

  Conditions: The symptom is observed when the standby tries to sync with the active and when "crypto pki trustpoint" is configured with an unavailable port-channel as source-interface.

  Workaround: There is no workaround.

- CSCti09284

  Symptoms: A Cisco device may display the following error messages in the logs when IPS is enabled:

  ```
  %SYS-2-CHUNKINVALIDHDR: Invalid chunk header type
  ```

  Conditions: The symptom is observed when IPS rulesets are enabled on the interfaces.

  Workaround: Remove IPS ruleset configuration from interface configurations.

- 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.

- CSCti17841

  Symptoms: Removing "match condition" from a class map crashes the router.

  Conditions: The symptom is observed when you remove "match condition" from a class map.

  Workaround: There is no workaround.

- CSCti19261

  Symptoms: A Cisco 87xW router and other routers with a wireless device will crash in rare cases when transmitting a packet.

  Conditions: The symptom is observed with normal traffic.

  Workaround: There is no workaround.

- CSCti25459

  Symptoms: Device might crash with fib_forw_add_extra_encap_and_forward. Also possibly seeing ICMP packets with unreachable sourced.

  Conditions: The symptom is observed when MLPS is enabled on these devices.

  Workaround: Use NAT NVI instead of legacy NAT.

- CSCti32334

  Symptoms: DDNS process gets stuck and marks all updates as duplicates. The command **debug ip dhcp server packet detail** shows:

```
DDNS: Duplicate update rejected 'host.somedomain.com.' <=> 192.168.0.1 server 0.0.0.0
```

Conditions: This happens in a day or so under moderate load following a router reboot. DDNS updates are performed by IOS DHCP server ("update dns" is configured in a pool).

Workaround: There is no workaround.

- CSCti34056

  Symptoms: If ISAKMP (P1) SA is lost but a valid IPSec SA (P2) still exists with a constant inbound data traffic being received from the peer, periodic DPD configuration does not re-trigger IKE and hence DPDs are not sent to the peer.

  Conditions: Router A and Router B are configured with LAN-to-LAN IPSec tunnel. Router B has "crypto isakmp keepalive 10 3 periodic" configured. Router B loses IKE SA, after which DPDs are not sent.

  Workaround: Execute a **clear cry sa** (P2) or **clear cry session** on Route B to reinitiate a new IKE P1.

- CSCti34968

  Symptoms: ACL with QoS is crashing the router, if one of the ACEs is evaluate or reflect.

  Conditions: The symptom is observed if the pure ACL used under a class-map is also a reflexive ACL. It is observed only in a pure QoS class-map configuration which has only access-group match filter. It is not seen with an impure QoS class-map configuration which has access-group as well as other filters like DSCP.

  Workaround: Do not use reflexive ACL under QoS. It is not a good practice.

- CSCti36310

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router is leaking memory when IKE attribute are pulled by SNMP.

  Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router with SNMP enabled. The leak has been observed with the asr1000rp1-adventerprisek9.03.01.00.S.150-1.S and asr1000rp1-adventerprisek9.02.06.01.122-33.XNF1 images.

  Workaround: There is no workaround.

- CSCti47995

  Symptoms:

  1. Traffic gets punted and dropped since CEF has stale state of prefix.
  2. IP complains of duplicate address:

```
%IP-4-DUPADDR: Duplicate address 192.168.0.101 on FastEthernet1/2, sourced by
0030.7bb9.f01e
```

  Conditions: The symptom is observed when there is NAT configured, traffic is flowing and then NAT is unconfigured.

  Workaround: There is no workaround.

- CSCti49372

  Symptoms: V.34 modem relay call connects for few seconds, shows a lot of garbage characters on originating and terminating hyperterminals, and then gets disconnected.

  Conditions: This is seen with external modems and MGCP gateways configured for V.34 modem relay.

  Workaround: There is no workaround.

- CSCti50607

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

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

  Workaround: There is no workaround.

- CSCti54127

  Symptoms: System crash.

  Conditions: The symptom is observed with the following conditions:

  1. Configure 12-in-1 serial in Async mode.
  2. Launch sweep pings (with incremental packet sizes) from the peer to UUT.
  3. Configure “mtu 64” on serial interface of UUT.
  4. Configure “default mtu” on serial interface of UUT.

  Workaround: Stop traffic or shut down the interface before modifying the MTU configuration.

- CSCti54149

  Symptoms: Fax machine sends out v29, signaling proprietary faxing.

  Conditions: The symptom is observed when sender and receiver are using same type of fax machine.

  Workaround: There is no workaround.

- CSCti54217

  Symptoms: Unexpected reload may occur with the following message:

  ```
  Unexpected exception to CPU: vector 1400, PC = 0x803445B8, LR = 0x803385C4
  ```

  Conditions: The symptom is observed on a Cisco 1812 router that is running Cisco IOS Release 12.4(15)T12.

  Workaround: There is no workaround.

- CSCti54671

  Symptoms: A SIP REFER sent to CUBE with SIP header Call-Info=<parameter data> is not passed to the outbound INVITE on CUBE. The data in SIP header Call- Info is lost.

  Conditions: This symptom is observed in a SIP environment supporting CVP, CUBE, and ICM. ICM sends instructions to CVP to add the Call-Info header to the REFER message. The Call-Info header contains data elements that need to be passed to a target system. CUBE is configured to consume the REFER, thereby generating an INVITE to send to the target system. The REFER process works as expected, i.e.: the INVITE is forwarded to the target system. But the Call-Info data element is lost in the transaction from REFER method to INVITE method.

  Workaround: There is no workaround if a REFER is used. However, if CVP sends an re-INVITE with SIP header Call-Info=<parameter data>, CUBE does forward the data element correctly to the target system.

- CSCti56560

  Symptoms: With bursty traffic, drops are seen in the interface drop counters that are not accounted for in the per-traffic-class counters. Furthermore, some of these unaccounted packet drops may occur in a traffic-classes where the offered rate is much less than the shape rate (i.e.: where the shaper is not active).

  Conditions: The symptom is observed with a hierarchical policy-map with shape in several parent traffic-classes and fair-queue in the child traffic class is applied to a POS interface.

Workaround 1: Set “hold-queue 4096 out” under the interface configuration mode. This will set up a maximal output buffer to make the driver more tolerant of bursts.

Workaround 2: Tune the shaper to eliminate excess bursts.

- CSCti58426

  Symptoms: A router may encounter a crash when the **show buffers usage** command is issued.

  Conditions: The symptom is triggered by the **show buffers usage** command.

  Workaround: Avoid running the **show buffers usage** command.

- CSCti58625

  Symptoms: When you issue the command **privilege voiceport level 2 shut** in a configuration terminal, the VG224 will become hung for over two hours. After the command is enabled, it also takes a long time to issue a **write memory** or **show run**.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T. Other releases may be affected.

  Workaround: There is no workaround.

- CSCti59419

  Symptoms: Double digits being sent (OOB and RFC2833).

  Conditions: The symptoms are observed if no DTMF method is specified in the CRCX from CA and when running Cisco IOS Release 12.4(25c) and above.

  Workaround: Use Cisco IOS Release 12.4(7c).

- CSCti59428

  Symptoms: TCP sessions stop working after a few days.

  Conditions: The symptom is observed when a TCP session has been opened for a long time, e.g.: for TCP SYSLOG use.

  Workaround: There is no workaround.

- CSCti59648

  Symptoms: Intermittently (approximately once every 4 or 5 calls), ISDN calls are disconnected by the Cisco MGCP gateway.

  Conditions: The symptom is observed because the CallManager times out waiting for CONNECT_ACK from the MGCP gateway (i.e.: T313 timer). The gateway does receive CONNECT_ACK from the PSTN almost immediately following the outgoing CONNECT. However, the gateway seems to encounter huge delays in back- hauling the CONNECT_ACK to CallManager.

  Workaround: Increase the “T313 timer” service parameter in Cisco Unified Communications Manager Administration page. Note that while this may alleviate the issue, the problem could still happen, perhaps less frequently.

- 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.

- CSCti63640

  Symptoms: A Cisco AS5400XM reloads due to:

  ```
  %SYS-6-STACKLOW: Stack for process Framer background.
  ```

  Conditions: The issue seen with Cisco IOS interim Release 15.1(02.14)T while booting up the router with ds0-group configurations (in startup config) for the controllers that are connected back-to-back in the same router.

  Workaround: There is no workaround.

- CSCti66153

  Symptoms: A Cisco 7200 series router with VSA in GETVPN deployment is logging 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 (e.g.: **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 (e.g.: **permit ip any any**).
  3. Have the Cisco 7200 in passive mode as well.
  4. Not using receive-only mode on the keyserver.

- CSCti66155

  Symptoms: A Cisco IPSec router may unexpectedly reload due to bus error or software-forced crash because of memory corruption or STACKLOW error.

  Conditions: This is seen when the WAN link goes down and causes recursion between multiple tunnels using tunnel protection. (That is, there are tunnel 0 and tunnel 1. After the WAN link goes down, the routing table shows a link to the tunnel 0 destination through tunnel 1 and the tunnel 1 destination is through tunnel 0.)

  Workaround 1: Change the tunnel source to be the physical WAN interface so that when the WAN link does go down, the tunnels are brought down immediately.

  Workaround 2: Change the routing protocol so that the router in question does not have recursive routing when the link goes down.

  Workaround 3: If possible, create a floating null route for the tunnel destinations that is less preferred than the route normal route to the tunnel destination, but more preferred than the route that gets installed after the WAN link goes down.

- CSCti67832

  Symptoms: Cisco 3900e platform router reloads while try to enable GETVPN Group Member (GM) all-features debugs.

  Conditions: The symptom is observed on a Cisco 3900e router that is running Cisco IOS interim Release 15.1(2.7)T and while trying to enable the debug **debug crypto gdoi gm all-features**.

  Workaround: There is no workaround.

- CSCti67905

  Symptoms: A Cisco router may experience a crash.

  Conditions: This has been experienced on Cisco routers running Cisco IOS Release 15.1(2)T and Release 15.1(2)T1. The routers are configured with IOS firewall and are inspecting FTP packets.

  Workaround: There is no workaround.

- CSCti69990

  Symptoms: A router crashes after deconfiguring IPv6 and then reconfiguring.

  Conditions: The symptom is observed only under specific conditions. Router has IPv6 configured on a number of interfaces and also has GLBP configured. IPv6 configuration is removed from all interfaces and then re-applied.

  Workaround: There is no workaround.

- CSCti71071

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

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

  Workaround: There is no workaround.

- CSCti75666

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

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

  Workaround: Convert H.323 leg to SIP.

- CSCti77384

  Symptoms: Traceback is seen while configuring DHCP on a virtual-template.

  Conditions: The symptom occurs during a PPPoE session.

  Workaround: There is no workaround.

- 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.

- CSCti79442

  Symptoms: One-way voice.

Conditions: The symptom is observed on a Cisco AS5400 MGCP controlled by PGW, SIP to PSTN call, with echo cancellation enabled. You see the RTP RX/TX counters increment with the **show call active voice brief** command.

Workaround: Explicitly define the MGCP codec type: **mgcp codec g711ulaw packetization-period 20**.

- CSCti79696

  Symptoms: A Cisco device may reload unexpectedly when a user edits content filtering settings through Cisco Configuration Professional (CCP).

  Conditions: The symptom is observed when editing content filtering settings through CCP.

  Workaround: Use command line instead of CCP.

- CSCti79848

  Symptoms: Router is running out of memory due to Chunk Manager.

  Conditions: The conditions are not confirmed at this time. It is believed to be related to Zone-based Firewall.

  Workaround: There is no workaround.

- CSCti82141

  Symptoms: The following symptoms are observed:

  1. The “none” option will be missing in the **show run** output after “ntp pps-discipline none inverted stratum <#value>” is configured.
  2. “Invalid input detected” error message will be thrown during the bootup and the configured “ntp pps-discipline none inverted stratum <#value>” will vanish after a reload.

  Conditions: The symptom is observed when the “inverted” option is included in the “ntp pps-discipline” CLI.

  Workaround: Configure the CLI without the “inverted” option.

- CSCti85446

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

  Conditions: The symptom is observed with the following conditions:

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

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

- CSCti88897

  Symptoms: When configuring the interface cellular 0 on a Cisco 880 series router that is running Cisco IOS Release 15.1(1)T1 or up to Release 15.1(2) T1, the command **service-policy output QOS_CUST_BASIC_OUT** disappears when the router is reloaded or power cycled.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(1)T1 or up to Release 15.1(2)T1.

  Workaround: There is no workaround.

- CSCti89532

  Symptoms: Classes in a policy-map are not getting the specified bandwidth for the class.

  Conditions: This happens when a bandwidth policy is attached to an ATM interface.

  Workaround: There is no workaround.

- CSCti89976

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

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

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

- CSCti91036

  Symptoms: Performance drop has been seen between Cisco IOS Release 15.1(1)T and Release 15.1(2)T.

  Conditions: The symptom is observed when you upgrade from Cisco IOS Release 15.1(1)T to Release 15.1(2)T.

  Workaround: There is no workaround.

- CSCti93175

  Symptoms: NAT router does not translate address of the last TCP ACK in the 3- way handshake.

  Conditions: The symptom is observed with the following conditions:

  - VRF NAT is involved.
  - “ip nat outside source translation” has to exist.
  - NAT flow-entries are disabled by **no ip nat create flow- entries**.

  Workaround: There is no workaround.

- CSCti93208

  Symptoms: HWIC-2SHDSL fails to train up with a third party vendor’s DSLAM.

  Conditions: This happens only if the board revision of the HWIC is C0.

  Workaround: Use a card with the board revision B0.

- CSCti93600

  Symptoms: Bus exception error is received due to a corrupted program counter.

  Conditions: The symptom is observed when a GigE link that is assigned to a port-channel is cleared and then followed immediately by a **show interface port-channel**.

  Workaround: If the **show interface port-channel** is done after the **clear interface** has completed (so that the GigE link is removed from the port-channel then added back in), the crash is not seen. In general, waiting 10 seconds between the **clear** and the **show** commands will avoid the crash.

- CSCti95511

  Symptoms: The command **no buffer header permanent** does not restore the default number of header buffers.

  Conditions:

  1. Issue is seen only when configuring header/fast switching buffers.
  2. Buffers need to be created for this pool.

Workaround: Configure the buffer CLIs carefully. This issue could be avoided by:

1. Not configuring “buffer header permanent” with a high value when available memory is low.
2. Not configuring “no buffer header permanent” when the number of buffers in the free list is less than the minimum value.

- CSCti95682

  Symptoms: CUBE crashes at sipSPICopySdpInfo if ReINVITE gets rejected for SRTP call.

  Conditions: The symptom is observed with the following conditions:

  – “srtp fallback” and “fax protocol pass-through g711ulaw” configured on CUBE.
  – Initial call establishes with SRTP and g729r8 codec.
  – CUBE receives a ReINVITE with RTP, g711ulaw codec and silenceSupp:off to switch to the fax passthru mode.
  – CUBE forwards the ReINVITE to the other end.
  – The other end rejects the ReINVITE with “488 Not Acceptable Media” error response (could be because fallback to RTP is not enabled or fax passthru is not enabled on the other end).
  – CUBE crashes after receiving 488 error response from the other end.

  Workaround: Configure uniform fax protocol (T38 or pass-through) and “srtp fallback” on all the gateways.

- CSCti96109

  Symptoms: Overall performance reduction on NAT.

  Conditions: The symptom is observed when NAT is enabled.

  Workaround: Revert to earlier images.

- CSCti96291

  Symptoms: AutoQoS-created class-maps get deleted from all policies when “no auto qos voip” is configured on any one DLCI.

  Conditions: The issue is seen on a Cisco 7200 series router that is running Cisco IOS interim Release 15.1(2.19)T0.1.

  Workaround: There is no workaround.

- CSCti97896

  Symptoms: A Cisco ISR router with 512MB of memory and iomem set to 25% may crash and hang at bootup.

  Conditions: The symptom is observed when booting a Cisco IOS 15.0 image with iomem set at 25% and 512MB of RAM.

  Workaround: Do not configure “memory-size iomem 25”. To restore from the hang you will need to physically reload the router, break to rommon, and issue the following rommon command: **iomemset smartinit**. Check that you have smartinit enabled using the rommon command **meminfo** which would show you “Smart Init is enabled”.

- CSCti98550

  Symptoms: A Cisco 870 router crashes upon an AnyConnect connection.

  Conditions: The symptom is observed on a Cisco 870 that is running Cisco IOS Release 15.1(1)T1. AnyConnect “client certificate authentication” is configured. The crash occurs when using AnyConnect 2.4 on the iPhone.

Workaround: Use username/password for authentication. Make sure “authorization username subjectname commonname” is configured under the trustpoint.

- CSCti99419

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

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

  Workaround: Power-cycle the router.

- CSCtj00039

  Symptoms: Some prefixes are in PE router EIGRP topology although those routes are not being passed to the CE router.

  Conditions: The symptom is observed when EIGRP is configured as a routing protocol between PE and CE routers.

  Workaround: Clear the route on the PE router using **clear ip route vrf** *xxx x.x.x.x*.

- CSCtj00728

  Symptoms: A router crashes when enabling a DECnet neighbor.

  Conditions: The symptom is observed with a DECnet neighbor limit on a single node of 32. If one exceeds 32, the crash is seen.

  Workaround: Limit neighbor count to 32.

- CSCtj01087

  Symptoms: CUBE advertises last negotiated payload size information in SIP-SDP after the call is held and retrieved. Call Flow: IP-Phone CUCM SIPIPIPGWSIPTelco:

  1. IP-Phone calls PSTN over SIP trunk and call connects - G729, 40ms payload size is negotiated.
  2. P-Phone puts caller on hold, and caller is connected with MOH - G711ulaw, 20ms payload is negotiated.
  3. IP-Phone retrieves the call - G279,20ms payload size is negotiated.

  Conditions: The symptom is observed on a Cisco 3945 router with the c3900-universalk9-mz.SPA.151-2.T.bin image. Voice-class codec is being used in Dial- Peer:

```
voice class codec 1
 codec preference 1 g711alaw
 codec preference 2 g711ulaw
 codec preference 3 g729r8 bytes 40

!
!Incoming Dial-Peer
!
!
dial-peer voice 2001 voip
 tone ringback alert-no-PI
 description Incoming from CISCO UCM
 huntstop
 preference 1
 session protocol sipv2
 incoming called-number .
 voice-class codec 1 offer-all
 no voice-class sip asserted-id
 voice-class sip privacy-policy passthru
 voice-class sip early-offer forced
 voice-class sip profiles 1
 dtmf-relay rtp-nte
```

```
 no vad
!
!Outgoing Dial-Peer
!
!
dial-peer voice 1001 voip
 tone ringback alert-no-PI
 description Outgoing to Prosodie
 translation-profile outgoing Outgoing_to_PSTN
 huntstop
 destination-pattern 0T
 session protocol sipv2
 session target ipv4:10.3.3.10
 no voice-class sip asserted-id
 voice-class sip privacy-policy passthru
 voice-class sip early-offer forced
 voice-class sip profiles 1
 codec g711alaw
 no vad
!
```

Workaround: Remove the voice-class codec and define the codec explicitly:

```
dial-peer voice 2001 voip
no voice-class codec 1 offer-all
codec g729r8 bytes 40 fixed-bytes
```

- CSCtj01235

  Symptoms: A crash is seen when running the command **debug crypto isakmp** during ISAKMP profile selection. The crashinfo file shows that the crash is happening during MM_KEY_EXCH as it receives the certificate from the remote peer.

  Conditions: The symptom is observed on a Cisco ASR 1000 Series Aggregation Services router that is running Cisco IOS Release 15.0(1)S.

  Workaround: There is no workaround.

- CSCtj01278

  Symptoms: The **show memory statistics** command show memory leaks:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of xxxx bytes failed from 0xyyyyyyyy, alignment 0
  Pool: Processor Free: xxxx Cause: Memory fragmentation Alternate Pool: None Free: 0
  Cause: No Alternate pool -Process= "Licensing Auto Update Process", ipl= x, pid= xx
  ```

  Conditions: The symptom is observed using the following command with options: **privilege route-map level x**.

  Example: **privilege route-map level 10 set extcommunity privilege route-map level 10 set interface**

  Workaround: There is no workaround.

- CSCtj02163

  Symptoms: DSP is not being released during voice call connection.

  Conditions: The symptom is observed with a hair-pin call across two ports in different slots.

  Workaround: There is no workaround.

- 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> ***.

- CSCtj05198

  Symptoms: When there are two EIGRP router processes (router eigrp 7 and router eigrp 80), PfR is unable to find the parent route. The problem occurs only if one of the processes has the parent route and other one does not. As a result, probe and route control fail.

  Conditions: This symptom is observed when there are two EIGRP router processes.

  Workaround: Use one EIGRP process. There is no workaround if two processes are used.

- CSCtj07885

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

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

  Workaround:

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

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

  b. Turn off SNMP polling on the device.

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

- CSCtj07904

  Symptoms: EIGRP neighbor relationship goes down with “no passive interface” configured.

  Conditions: The symptom is observed when “no passive interface” is configured.

  Workaround: Do not configure “passive-interface default” and allow the interface to be non-passive by default. Configure “passive-interface <interface>” for the interface to be passive.

- CSCtj08368

  Symptoms: Router software crash at process_run_degraded_or_crash.

  Conditions: The symptom is observed when the allocated memory block is freed.

  Workaround: There is no workaround.

- CSCtj08533

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

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

  Workaround: Use only one path between PE and CPE.

- CSCtj08869

  Symptoms: Router crash seen when LAT is disabled.

  Conditions: This is seen on a Cisco 7200 series router loaded with Cisco IOS interim Release 15.1(2.18)T.

  Workaround: There is no workaround.

- 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.

- CSCtj10592

  Symptoms: DVTI GRE IPv4 mode fails to create virtual-access for IKEv2 connections.

  Conditions: The symptom is observed with a simple SVTI to DVTI connection.

  Workaround: There is no workaround.

- CSCtj11346

  Symptoms: VSA IPSec card can not process encrypted data from peer.

  Conditions: The symptom is observed when you enable the VSA card.

  Workaround 1: Replace the router (third-party equipment) with a Cisco router.

  Workaround 2: Disable the VSA with **no crypto engine slot 0**.

- CSCtj11682

  Symptoms: An HWIC-3G-CDMA-S modem slows down to 1xRTT speed and does not recover when 1xEVDO service is available.

  Conditions: The symptom is observed when 1xEVDO service is interrupted and the modem goes to the 1xRTT service that is available. When 1xEVDO service returns, the modem does not return to the higher rate service.

  Workaround: The following EEM script can be utilized as a workaround for the Cisco 880 series of routers that utilize the PCEX cards. It can be modified to work with the 1800 and larger series of routers that utilize the HWIC cards also:

  ```
  event manager applet WA
   event syslog pattern "%SYS-5-RESTART"
   action 1.1 wait 15
   action 1.2 syslog msg "Applying Service-policy to the Async interface"
   action 2.1 cli command "enable"
   action 2.2 cli command "lab"
   action 2.3 cli command "config terminal"
   action 2.4 cli command "int cell 0"
   action 2.5 cli command "service-policy output TEST"
   action 2.6 cli command "end"
   action 2.7 cli command "write memory"
   action 3.1 syslog msg "Service policy has been configured on the Async
  interface"
  ```

- CSCtj13210

  Symptoms: Memory leaks are observed at **ipsec_db_add_gdoi_sa_req** on GETVPN keyservers.

  Conditions: This symptom is observed with GETVPN keyservers when a large amount of traffic is sent between GETVPN GMs.

  Workaround: There is no workaround.

- CSCtj14738

  Symptoms: Router crash. Before the crash we see the following error messages:

  ```
  %ISDN-6-DISCONNECT: Interface Serial0/0/0:4 disconnected from 6406418 , call lasted
  1410 seconds
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x244, pc=0x247BE87Cz ,
  ra=0x247BE878z , sp=0x3175D388
  ```

  Conditions: The symptom is observed on a Cisco 2911 router that is running the c2900-universalk9-mz.SPA.150-1.M1.bin image.

  Workaround: There is no workaround.

- CSCtj15798

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

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

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

- CSCtj15884

  Symptoms: One-way voice when SRTP is used.

  Conditions: The symptom is observed when interworking with PGW.

  Workaround: There is no workaround.

- CSCtj16036

  Symptoms: A Cisco router may experience a crash due to a watchdog timeout after seeing CPUHOG messages.

  Conditions: This has been experienced on a Cisco 7206XR that is running Cisco IOS Release 12.4(24)T3. The router is configured with PPP interfaces.

  Workaround: There is no workaround.

- CSCtj16291

  Symptoms: Voice router crashes due to memory corruption.

  Conditions: The symptom is observed when multiple SIP Register are received. The response causes a Send Error.

  Workaround: There is no workaround.

- CSCtj17425

  Symptoms: Router configured for SSL VPN crashes.

  Conditions: The symptom is observed when SSL VPN is configured.

  Workaround: There is no workaround.

- CSCtj18622

  Symptoms: The “qos_peruser” feature is not working when it is pushed through AV_Pair by a RADIUS server; either Cisco ACS or a third party vendor’s server.

  Conditions: The symptom is observed with non-multilink PPP users.

  Workaround: There is no workaround.

- CSCtj20163

  Symptoms: On a PE1-P-PE3 setup, a crash is seen on P (core) router with scaled MLDP configurations.

  Conditions: The symptom is observed with the following conditions:

  1. Execute **show mpls mldp database**.
  2. Reload Encap PE.
  3. Crash seen on P router when MLDP neighbors go down.

  Workaround: There is no workaround.

- CSCtj20588

  Symptoms: Router hangs and generates crashinfo files upon reboot after removing an access-list used in a class-map via this command: **no ip access-list <name>**. The following error message is logged prior to the crash:

  ```
  %SYS-3-CPUHOG:Task is running for (120004)msecs, more than (2000)msecs
  (976/266),process = SNMP ConfCopyProc.
  ```

  Also, spurious access (%ALIGN-3-SPURIOUS) could be seen (without crashing the router) when that command is entered.

  Conditions: The symptom is observed on a Cisco 3845 router after upgrading to Cisco IOS Release 15.1(2)T1.

  Workaround: Avoid removing access-lists.

- CSCtj20634

  Symptoms: Normal door not getting created.

  Conditions: The symptom is observed while sending H225 packets across UUT.

  Workaround: There is no workaround.

- CSCtj21045

  Symptoms: Header compression decodes RTP timestamp incorrectly.

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

  Workaround: Use IETF format compression.

- CSCtj21120

  Symptoms: CPUHOG for process “IP SLAs XOS Event Processor” is seen followed by a router crash. After the router is reloaded, it then crashes again with the same decode.

  Conditions: The symptom is observed when the router is configured with two external interfaces with total of 3200 appls prefix with 50 OER maps and 64 appls prefix in each OER map in fast mode.

  Workaround: There is no workaround.

- CSCtj21327

  Symptoms: IP addresses are getting NATed properly, but the content-length is not being changed and the resulting packets are rejected by a firewall (due to the content length not being updated).

  Conditions: The NAT router is a Cisco 2921 router running Cisco IOS Release 15.0(1)M1 and doing static NAT and NATTING for embedded addresses in SIP packets.

  Workaround: There is no workaround

- CSCtj21696

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

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

```
OMHQ-C2800-49#sho inv
NAME: "chassis", DESCR: "2801 chassis"
PID: CISCO2801          , VID: V04 , SN: FTX1149Y0KF

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

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

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

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

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

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

- CSCtj23189

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

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

  Workaround: There is no workaround.

- CSCtj28747

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

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

  Workaround: There is no workaround.

- CSCtj32914

  Symptoms: CU is getting an error message, spurious memory access, and traceback:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x801697CCz reading 0x0
```

  Conditions: The symptom is observed on a Cisco 1861-UC-2BRI-K9 that is running Cisco IOS Release 15.0(1)M3.

  Workaround: There is no workaround.

- CSCtj32920

  Symptoms: Packet drop seen while pinging from UUT to Pagent through VLAN.

Conditions: The symptom is observed on a router that is running Cisco IOS interim Release 15.1(3.1)T.

Workaround: There is no workaround.

- CSCtj34061

  Symptoms: System reloads during a conference call that is established between an analog/FXS endpoint and SIP phones (SPA 50x/30x).

  Conditions: The symptom is seen under the following conditions:

  1. Analog phone calls SPA-1 phone.
  2. Press flash on the analog phone and call SPA-2 phone.
  3. After SPA-2 answers, press flash to conference all phones.

  Workaround: There is no workaround.

- CSCtj35106

  Symptoms: Spurious memory access seen:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x61CBC400z reading 0x70
%ALIGN-3-TRACE: -Traceback= 0x61CBC400z 0x631A1ABCz 0x63156BA0z 0x631A508Cz
0x631A5600z 0x62B75A10z 0xFFFF95C0z 0xFFFF95C0z
0x61CBC400:ipv6_enqueue(0x61cbc3dc)+0x24
0x631A1ABC:fw_dp_insp_send_rsts(0x631a00b8)+0x1a04
0x63156BA0:fw_dp_tcp_inactivity(0x631567ac)+0x3f4
0x631A508C:fw_dp_insp_handle_sis_idle_timeout(0x631a4c64)+0x428
0x631A5600:fw_dp_insp_handle_timer_event(0x631a554c)+0xb4
0x62B75A10:tw_notify(0x62b75944)+0xcc
```

  Conditions: The symptom is observed with any self-generated IPv6 traffic.

  Workaround: There is no workaround.

- CSCtj35148

  Symptoms: On a Cisco 3945, configuration for more than 256 dialer interfaces is disallowed.

  Conditions: The symptom is observed with more than 256 dialer interfaces configured.

  Workaround: Configure dialer maps with rotary-groups (we do not know the scale numbers for this and whether it will support say, 512 maps per interface).

- CSCtj35792

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

  Conditions: This symptom is observed when the onboard GE is connected by fiber to a gig port that is not doing autonegotiation.

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

  The Cisco 3945-E does not have this problem.

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

- CSCtj38234

  Symptoms: IPSec IKEv2 does not respond to INVALID_SPI informational message. It should respond with another INFORMATIONAL IKE message.

  An INVALID_SPI may be sent in an IKE INFORMATIONAL exchange when a node receives an ESP or AH packet with an invalid SPI. The notification data contains the SPI of the invalid packet. The INVALID_SPI message is received within a valid IKE_SA context.

Conditions: The symptom is observed when an IKEv2 peer sends an INFORMATIONAL IKE message notifying about an INVALID_SPI (IPSec).

Workaround: There is no workaround.

- CSCtj38492

  Symptoms: Hold resume fails when there is a redirected call from CUCM transit via CUBE.

  Conditions: The symptom is observed with CUCM 7.1.

  Workaround: There is no workaround.

- CSCtj38519

  Symptoms: EIGRP pacing timer is large when there is a large number of peers on NBMA interfaces.

  Conditions: The symptom is observed when EIGRP is configured with a large number of peers on a single NBMA interface.

  Workaround: Ensure spokes are setup as stub and properly summarized.

- CSCtj39558

  Symptoms: Sub-interface queue depth cannot be configured.

  Conditions: The symptom is observed when the policy is attached to ethernet subinterfaces.

  Workaround: There is no workaround.

- CSCtj39777

  Symptoms: A Cisco 2921 router crashes with IPSec and QoS.

  Conditions: The symptom is observed on a Cisco 2921 router when QoS pre-classify is enabled.

  Workaround: There is no workaround.

- CSCtj41867

  Symptoms: A Cisco 2900 Integrated Service router that is running Cisco IOS Release 15.1(2)T exhibits increased memory utilization over time.

  Conditions: The symptom is observed when a Cisco 2900 Integrated Services router that is running Cisco IOS Release 15.1(2)T is configured as a branch router that has an VPN WAN connection, Quality Of Service (QoS) classification configured (“qos pre-classify”), and WAAS Express enabled on a several interfaces with MLPPP enabled.

  Workaround 1: Disable QoS classification on VPN tunnel interface.

  Workaround 2: Disable WAAS Express on VPN tunnel interface.

  Workaround 3: Reduce the number of serial interfaces down to one

  Further Problem Description: The symptom is not observed when QoS classification is not configured or when MLPPP is not configured or when WAAS Express is not enabled.

- CSCtj44343

  Symptoms: The output from commands executed using the **exec** Tcl command cannot be saved into variables. Instead, the output is redirected to the terminal.

  Conditions: This occurs after running a Tcl script a number of times. For example, the issue has been seen after running a Tcl script four times. After the fourth time the output will not be saved in variables.

  Workaround: There is no workaround.

- CSCtj44520

  Symptoms: System crashes with memory block corruption.

  Conditions: The symptom is observed when running traffic with QoS, crypto, tunneling, and MLPP features enabled.

  Workaround: Remove one of the features.

- CSCtj46670

  Symptoms: When a dialer interface has moved out from standby mode when the primary link is up, you cannot open LCP since you reply with an IPCP CONFREJ. Also dialer string is needed to be configured for PPPoX scenario, as per debug dialer events.

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

  Workaround: Reload the router.

  Further Problem Description: When enabling dialer debugs the following error message is seen:

  Di1 DDR: Cannot place call, no dialer string set

- CSCtj46843

  Symptoms: Gateway detects the fax tone but does not initiate NSE packets towards the originating gateway.

  Conditions: The symptom is observed on a Cisco 3945 router that is running Cisco IOS Release 15.0(1)M3 and with DSP code: 26.3.7.

  Workaround: There is no workaround.

- CSCtj47696

  Symptoms: A Cisco 3845/3925 router 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 or 3900 series router with NM-8CE1T1-PRI or HWIC-2CE1T1-PRI that is running Cisco IOS Release 15.1 (1)T or Release 12.4(24)T4 deriving the clock from the network.

  Workaround: Configure local clocking (“no network-clock-participate”) and reload.

  Further Problem Description: With “no network-clock-participate” configured, a call will succeed on ISDN layer but an analog call will fail due to lack of synchronization between the PVDM and the PRI.

- 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 configs:

```
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 configs:

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

- CSCtj48242

  Symptoms: A memory leak is seen in the processor memory. The **show mem debug leaks summary** command shows that “Presence Process” and “mem_mgr: mem_mgr_malloc_buf” is leaking.

  Conditions: The conditions are not fully known yet. It looks like the issue is related to SIP traffic.

  Workaround: There is no workaround.

- CSCtj48629

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

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

  Workaround: There is no workaround.

- CSCtj48913

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

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

  Workaround: There is no workaround.

- CSCtj49133

  Symptoms: After attaching a policy-map to a sub-interface, the policy-map is then renamed and then the sub-interface is deleted. The policy-map definition can not be deleted and still shows up in the running configuration.

  Conditions: The symptoms are observed with the following steps:

  1. Attach a policy to a sub-interface.
  2. Rename the policy-map.
  3. Remove the sub-interface.
  4. Removing the definition of policy-map will not succeed.

  Workaround: Remove the service policy from sub-interface before removing the sub-interface.

- CSCtj49957

  Symptoms: Multicast source NAT translation does not work correctly with simultaneous replication to both inside and outside interfaces.

  Conditions: The symptom is observed when replicating the multicast feed from a NAT inside interface to both a NAT inside and outside interface simultaneously. The intended result: translated packets to the outside interface being translated but not packets to the inside interface.

  Workaround: There is no workaround.

- CSCtj52795

  Symptoms: Crash is seen when unconfiguring the service policy under the tunnel interface.

  Conditions: The symptom is observed when the tunnel interface comprises NAT and multicast configurations.

  Workaround: There is no workaround.

- CSCtj53363

  Symptoms: Router hangs and console does not respond indefinitely.

  Conditions: The symptom is observed with the following conditions:

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

  Workaround 1: If running a Cisco 2811/2821, use sw crypto + ZBFW.

  Workaround 2: If running with a Cisco 2851 and higher ISRs, use onboard crypto + VPN instead of AIM-VPN + ZBFW.

- CSCtj53407

  Symptoms: When WAN interfaces of 860, 880, and 890 are configured for fixed speed/duplex settings (100/full, 100/half, 10/full, 10/half), the link goes down. Autonegotiation works fine.

  Conditions: Both the ends of the link should be configured for fixed speed/duplex settings.

  Workaround: There is no workaround.

- CSCtj54666

  Symptoms: IP jitter statistics table is corrupted when rttMonApplTimeOfLastSet rolls over the 32 big mark.

  Conditions: The symptom is observed with the IP jitter statistics table.

  Workaround: There is no workaround.

- CSCtj55834

  Symptoms: Input drops seen when “queue-limits” are applied.

  Conditions: The symptom is observed when using traffic policing and queue limits in a child policy-map. This occurs when the configured queue-limit is much higher than the default of 64 and may be due to buffer starvation.

  Workaround: Use a lower value or the default of 64.

- CSCtj56519

  Symptoms: Multicast over VMI in NBMA-mode fails with IGMPv3.

  Conditions: This issue is seen in routers loaded with Cisco IOS interim Release 15.1(2.19)T0.1.

  Workaround: There is no workaround.

- CSCtj58458

  Symptoms: A Cisco IAD887 fails to respond because of an IO buffer leak.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(1)T.

  Workaround: Reload the router.

- CSCtj58489

  Symptoms: Path confirmation failure for DO-EO with VCC and HD configurations.

  Conditions: The symptom is observed with a DO-EO with HD Transcoding and VCC configured. The following cases are failing because of this issue:

  ```
  BC_DO-EO_FA_VCC_SS_ReINV_HD
  BC_DO-EO_FT_VCC_SS_ReINV_HD
  BC_DO-EO_FA_VCC_EQ_ReINV_HD
  BC_DO-EO_FT_VCC_EQ_ReINV_HD
  ```

Workaround: There is no workaround.

- 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.

- CSCtj61284

  Symptoms: NAT overload does not work for non-directly connected destinations in MPLS-VPN configurations.

  Conditions: The symptom is observed with NAT overload configured to NAT traffic coming over an MPLS VPN to internet (via a VRF-enabled interface).

  Workaround: There is no workaround.

- CSCtj61657

  Symptoms: IO memory leak is seen followed by TCP no buffer logs:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of xxxx bytes failed from 0xXXXXXXXX, alignment
  xxx Pool: I/O Free: xxxx Cause: Not enough free memory Alternate Pool: None Free: 0
  Cause: No Alternate pool -Process= "Pool Manager"
  %TCP-6-NOBUFF: TTY0, no buffer available -Process= "SCCP Application", ipl= 0, pid=
  XXX
  ```
  Conditions: The symptom is observed in the presence of VOIP phones using multicast applications with the **session protocol multicast** dial-peer configuration command.

  Workaround: There is no workaround.

- CSCtj63307

  Symptoms: GRE fragments get dropped.

  Conditions: The symptom is observed with GRE fragments. The parent bug is CSCsv68549.

  Workaround: There is no workaround.

- CSCtj63943

  Symptoms: There is a router crash on applying **tunnel mode ipsec ipv4** under a tunnel interface.

  Conditions: The symptom is observed when the tunnel interface is up while configuring the command.

  Workaround: There is no workaround.

- CSCtj66235

  Symptoms: A UC540 that is running Cisco IOS Release 15.1(2)T1 reloads due to software-forced crash while experiencing the following error:

  ```
  %SYS-6-STACKLOW: Stack for process voice file acct dump running low, 0/6000
  ```
  Conditions: The crash suggests that the issue is just one of inefficient stack usage.

  Workaround: There is no workaround.

- 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.

- CSCtj67047

  Symptoms: While testing “PPP Cell Phone Negotiation” (MLP CEF switching), you may be unable to retrieve the total count of packets that are CEF-switched.

  Conditions: This issue is seen in a router that is loaded with Cisco IOS interim Release 15.0(1)M3.11.

  Workaround: There is no workaround.

- CSCtj67845

  Symptoms: A Cisco 2951 router crashes on power up.

  Conditions: The symptom is observed on a Cisco 2951 router when an HWIC-ADSL and EHWIC-VA-DSL are plugged in together.

  Workaround: There is no workaround.

- CSCtj69577

  Symptoms: When congestion occurs on a QoS-enabled output interface, output rate significantly decreases.

  Conditions: The symptoms are observed under the following conditions:

  1. 3945E outbound interface is connected to 100M link.
  2. QoS (LLQ/Fair Queue) is configured on 3945E outbound interface.
  3. Congestion occurs on outbound interface.

  Workaround: Reload the router.

  Further Problem Description: This issue is resolved after a reload but the shutdown/no shutdown commands can cause the same issue.

- CSCtj72592

  Symptoms: Crypto engine drops packets.

  Conditions: The symptom is observed on a Cisco 3900 that is running Cisco IOS Release 15.1(2)T with an output service-policy.

  Workaround: Remove QoS.

- CSCtj76297

  Symptoms: Router hangs with interoperability of VM and crypto configurations.

  Conditions: The symptoms are seen only during interoperability between video-monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

  Workaround: Disable AIM and use onboard CE.

- 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.

- CSCtj77477

  Symptoms: High LLQ delay.

  Conditions: The symptom occurs only on G.SHDSL EFM platforms 888E and ISR with HWIC-4SHDSL-E. There is high delay in priority queue when using CBWFQ/LLQ. For example:

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

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

```
EFM rate 2304 kbps

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

- CSCtj77819

  Symptoms: When dialer idle-timeout is not explicitly configured on a dialer interface (with PPP multilink configuration), then it is not effective. It is not resetting the idle timeout when outgoing interesting traffic is seen.

  Conditions: The symptom is observed when dialer idle-timeout is not explicitly configured on a dialer interface (with PPP multilink configuration).

  Workaround: Reconfigure “dialer idle-timeout” with any value (even default of 120 secs).

- CSCtj78107

  Symptoms: A Cisco 87X series router may show this message:

```
%OCE-3-OCE_FWD_STATE_HANDLE with SW Crypto
```

  When this message occurs, the router stops passing any traffic and has to be rebooted.

  Conditions: The symptom is observed when the router is running the software encryption engine. Every couple of days the following message appears on the console:

```
Limit of oce forward state handle allocation reached; maximum allowable number is
50000
```

  Workaround: Disable CEF (causes CPU spikes).

- CSCtj78210

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

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

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

  For example, configure:

```
voice-card 0 (1... 2... etc...)
dspfarm
dsp service dspfarm
```

```
dspfarm profile x conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown

dspfarm profile x2 conf
max sessions xx << use the maximum
max partic << use the maximum
associate app sccp
no shutdown

dspfarm profile x3 conf
max sessions xx << use maximum (if allowed)
max partic << use the maximum (if allowed)
associate app sccp
no shutdown

dspfarm profile x conf
shutdown
no dspfarm profile x conf
```

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

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

- CSCtj78407

  Symptoms: Router crashes.

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

  Workaround: A reload of the router fixes this issue temporarily.

- CSCtj78836

  Symptoms: A Cisco 3900 series router may undergo a software-forced reload.

  Conditions: This condition is observed with Cisco IOS interim Release 15.1 (2.19)T0.4, and only when Video Monitoring (VM) policy is configured.

  Workaround: Do not configure a VM policy.

- CSCtj79368

  Symptoms: All keyservers crash after removing RSA keys before changing to new ones based on security concerns.

  Conditions: The symptom is observed when removing RSA keys.

  Workaround: Stay on the same RSA keys.

- CSCtj79476

  Symptoms: Traffic loss and VLAN related errors seen when the traffic is sent for a prolonged duration on an HWIC-4ESW.

  Conditions: The symptom is observed when traffic is sent for a prolonged duration (>12hrs) on an HWIC-4ESW.

  Workaround: There is no workaround.

- CSCtj79480

  Symptoms: High CPU usage due to time_it (in interrupts).

Conditions: The conditions are undetermined at this time.

Workaround: Reload the router and the CPU goes down for certain time.

- CSCtj79761

  Symptoms: All bearer channels in T1 PRI are not engaged.

  Conditions: The symptom is observed when dialer is configured and more than T1 line rate traffic is sent.

  Workaround: There is no workaround.

- CSCtj79765

  Symptoms: Attributes downloaded from AAA server are not applied to UUT.

  Conditions: The symptom is observed with attributes downloaded from AAA server.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.1(3)T

All the caveats listed in this section are resolved in Cisco IOS Release 15.1(3)T. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsb14936

  Symptoms: SNMPv3 gets/sets fail following a PRE switchover. Attempts increment usmStatsWrongDigests.0.

  Conditions: This symptom is observed in configurations with RPR+ and that use SNMPv3, where the snmp EngineID value is the default value.

  Workaround: The workaround for this symptom is to specify a value for the snmp EngineID via the global configuration cli “snmp-server engineID local [octet string],” where octet string is the desired engineID value.

  Further Problem Description: Once the device is upgraded to an image that has this fix, and if the device does not have “snmp-server engineID local [octet string]” configured, then all the existing v3 authNoPriv/authPriv users will not work. The v3 authNoPriv/authPriv users will have to be reconfigured.

- 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.

- CSCsk82537

  Symptoms: About once every 1 or 2 minutes, the value of the delta time found in the responding router in an IP SLA setup is 1 second behind the value it should have. This is causing false timeout as the RTT is then considered as being around 24 hours. The following output illustrates this problem:

  ```
  IP SLAs(100) jitter operation: Timed out arrival (rtt=86399012)
  For 3 consecutive probes:
  ```

```
ST: 75656998, RT: 75657005, DT: 0, CT: 75657014 => correct ST: 75658006, RT: 75658009,
DT: 0, CT: 75657018 => should be 75658018 ST: 75659006, RT: 75659009, DT: 0, CT:
75658018 => should be 75659018 ST: 75659998, RT: 75660005, DT: 0, CT: 75660014 =>
correct
```

Conditions: This has been seen on a Cisco 1812 running Cisco IOS Release 12.4(6)T7.

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.

- CSCso20810

  Symptoms: A buffer leak may occur when a router is configured with the combination of NAT, multicast and encryption. This occurs when multicast subsequently flows out a crypto-enabled interface.

  Conditions: This symptom will effect only those users whose routers are part of a multicast group. They must also have NAT and crypto configured on one or more of the interfaces in the multicast group.

  Workaround: Multicast traffic can be forwarded via a GRE tunnel instead of in the clear.

- CSCsu95339

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

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

  Workaround: There is no workaround.

- 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 seen on Ethernet.

- CSCsz79652

  Symptoms: A memory leak may be seen in Dead memory.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(50)SE and Release l2.2(50)SE1. Cisco IOS Release 12.2(44)SE is not affected. The symptom occurs when using Cisco Network Assistant to poll the device. The **ip http server** command or **ip http secure- server** command must be enabled for the leak to occur.

  Workaround: Disable the http server or stop CNA from polling the device.

- CSCta53372

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

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

  Workaround: Reset the RRI session.

- CSCta79941

  Symptoms: A virtual interface is not created when invoked using the **ip unnumbered** *type number* command.

  Conditions: This symptom is observed under a PPP interface when the virtual interface has been previously deleted.

  Workaround: Recreate the virtual interface manually using the **interface** command.

- CSCta91928

  Symptoms: A Cisco 881GW with a 3G modem may crash when the modem is reset or power-cycled.

  Conditions: This symptom is observed on a Cisco 501 or 880 with a 3G modem when “test cellular 0 modem-power-cycle” or “test cellular 0 modem-reset” is entered.

  Workaround: There is no workaround.

- CSCtb55576

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

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

  Workaround: There is no workaround.

- CSCtb57180

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

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

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

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

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

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

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

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

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

1. Avoid nested VTY access. For example, RouterA->RouterB->RouterA->RouterB.
2. Avoid issuing the **clear vty** command or the **clear line** command when there is any nested VTY access.
3. Avoid issuing the **clear vty** command or the **clear line** command when there are multiple VTY accesses from the same host.
4. Avoid issuing the **clear vty** command or the **clear line** command when router CPU utilization is high.
5. Avoid issuing the **show users** command repetitively in a short period of time.

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

- CSCtb69063

  Symptoms: Memory corruption occurs when a user name is configured to a maximum length of 64 characters, as shown:

  ```
  config# username <name of 64 characters> priv <0-15> password 0 <password>
  ```

  Conditions: The symptom is observed if the user name is exactly 64 characters.

  Workaround: Configure a user name of 63 characters or less.

  Further Problem Description: When some configurations are added, modified, or deleted the **show configuration id detail** command prints information of last change time, changed by user, and changed from process. If the user name is very large (exactly 64 characters), then the “changed by user” field prints unwanted characters.

- CSCtb89424

  Symptoms: In rare instances, a Cisco router may crash while using IP SLA udp probes configured using SNMP and display an error message similar to the following:

  ```
  hh:mm:ss Date: Address Error (load or instruction fetch) exception, CPU signal 10, PC
  = 0x424ECCE4
  ```

  Conditions: This symptom is observed while using IP SLA.

  Workaround: There is no workaround.

- CSCtc33679

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

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

  Workaround: There is no workaround.

- CSCtc52299

  Symptoms: UDP packets broadcast with destination port 53 for 10 minutes bring the CPU to 100% and cause a router crash if the dns server is removed.

  Conditions: This symptom is observed with UDP broadcast at port 53, which causes the port to remain open and the CPU hog to occur in 5-10 minutes. The router CPU reaches 100% capacity and does not come down even after the broadcast traffic is stopped.

  Workaround: There is no workaround.

- CSCtc55897

  Symptoms: R2 will not advertise the routes.

  Conditions: The symptom is observed under the following conditions:

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

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

- CSCtc58917

  Symptoms: Dialer idle timeout is not being reset with interesting traffic.

  Conditions: This symptom is observed when MPPC compression is turned on.

  Workaround: There is no workaround.

  Further Problem Description: A call is made from Windows XX client dial-up networking to the NAS. After the call is established and interesting traffic is sent every 30 seconds for 180 seconds, idle timeout is not being reset.

- CSCtc71408

  Symptoms: Fax transmission fails when CUBE is in the middle.

  Conditions: The symptom is observed when either one of the dial-peers on OGW/TGW/CUBE is configured for fax protocol T38 version 0.

  Workaround: Configure version 3 on all dial-peers.

- CSCtc78200

  Symptoms: A Cisco router may crash in the parse_configure_idb_extd_args routine.

  Conditions: This symptom is observed when running PPP sessions or when TCL is used for configuring interface range.

  Workaround: As PPP session is being established on the LNS, IOS will momentarily use one of the available VTYs from the router. After initial configuration is done, it is immediately released to the system pool.

  If all VTY connections are in use, then we will see an RP crash if a new PPP session is being established and there are no free VTYs in the system.

  To work around this issue, reserve several VTY connections for PPP session establishment. Since it is possible that a burst of PPP sessions tries to connect thereby using multiple VTY connections at the same time, it is recommended to reserve at least 5 VTY connections. One possible solution is to use an ACL on the last 5 VTY lines:

  ```
  ip access-list extended VTY_ACL deny ip any any ! line vty 5 9 access-class VTY_ACL
  in exec-timeout 1 0 login authentication local1
  ```

  Alternate Workaround: Do not configure “interface range” cli using ios_config from tclsh mode. When in tclsh mode, use normal “interface cli” in a “for loop.”

- CSCtd30544

  Symptoms: Netflow is showing Null in the destination interface even though packets are not getting dropped or blocked.

Conditions: This symptom is seen when connected to the LNS via VPDN and browsing HTTP. Intermittently Null output is seen as the destination interface as the packet being punted between different CEF switching paths due to **ip tcp adjust-mss** *value* configuration that is applied on the destination interface.

Workaround: Remove **ip tcp adjust-mss** *value* from the destination interface.

- 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.

- 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.

- CSCtd54301

  Symptoms: A Cisco router gets struck in syntax-conf-ssh-pubkey-data mode, and you are not able to exit from syntax-conf-ssh-pubkey-data mode.

  Conditions: This symptom is observed on a Cisco 7200 router loaded with a Cisco IOS 15.1(0.17)T image.

  Workaround: There is no workaround.

- CSCtd59027

  Symptoms: A Cisco 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 have 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 affect 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.

- 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.

- CSCte17560

  Symptom: Offered rate in QoS class shows unusually high values.

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

  Workaround: There is no workaround.

- CSCte18124

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

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

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

- CSCte20187

  Symptoms: When bgp next-hop is configured under a VRF, the following error message is seen on the remote PE router:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (1)
  ```

  The label advertised may be different but it is always a reserved label (0- 15).

  Additionally, the local PE will see “No Label” as the Outgoing Label” in the MPLS forwarding table.

  Conditions: This symptom is observed when bgp next-hop is configured under an interface.

  Workaround: There is no workaround.

- CSCte27828

  Symptoms: Call forward does not work.

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

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

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

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

  Workaround: There is no workaround.

- CSCte61495

  Symptoms: The following messages are seen with tracebacks:

  ```
  %SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs (4/4),process
  = Exec. %SYS-2-INTSCHED: ’suspend’ at level 3 -Process= “Exec”, ipl= 3, pid= 128,
  ```

  Conditions: The symptom is observed when a large ACL is configured for the service-policy. This happens only under ATM subinterfaces.

Workaround: Use small sized ACLs for the service-policy.

- CSCte82226

  Symptoms: While changing the MTU on a Port-channel, you may see the following traceback:

  ```
  SYS-SP-2-NOBLOCK error
  ```

  Conditions: This symptom is observed when changing the MTU on a Port-channel.

  Workaround: There is no workaround.

- CSCte85961

  Symptoms: The router crashes while doing a **shut** command followed by the **no shut** command to the main interface.

  Conditions: The issue is seen with scale configuration and giving the **shut** command followed by the **no shut** command in the main ATM interface.

  Workaround: There is no workaround.

- CSCte86038

  Symptoms: High CPU utilization for ATM OAM timer process.

  Conditions: The symptom is observed with a scaled L2 VC configuration.

  Workaround: Increase the AIS RDI timeout with higher number of up and down retries.

- CSCte89130

  Symptoms: Router experiences a memory leak.

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

  Workaround: There is no workaround.

- CSCte91259

  Symptoms: A Cisco router may unexpectedly reload due to a bus error after displaying an "%IDMGR-3-INVALID_ID" error.

  Conditions: The crash will be seen only if the router is using DHCP Client Dynamic DNS update.

  Workaround: There is no workaround.

- CSCte92581

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

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

  Workaround: There is no workaround.

  Further Problem Description: The stuck VRF cannot be reused.

- 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.

- CSCte94301

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

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

Workaround: There is no workaround.

- CSCte95301

  Symptoms: Memory leak in proxy authentication scenario, when authentication fails.

  Conditions: The symptom is observed when HTTP proxy authentication is used.

  Workaround: There is no workaround.

- CSCtf06436

  Symptoms: Continuous high CPU usage.

  Conditions: The symptom occurs after the formation of a recursion loop in the FIB, when the prefixes in the loop are labeled.

  Workaround: There is no workaround.

- CSCtf25293

  Symptoms: SSH connection to a SSH server aborts abruptly after making the connection, while using public key-based authentication.

  Conditions: Authentication method used must be public key.

  Workaround: Use kbd-interactive or password-based authentication.

- CSCtf35006

  Symptoms: If there are two jobs in an SNMP job queue and if you try to destroy the jobs, the console hangs.

  Conditions: The symptom is observed if you prepare multiple license action entries and then let them execute immediately.

  Workaround: There is no workaround.

- CSCtf40025

  Symptoms: “IP SLAs XOS Event Processor” process hangs and input queue of an interface is stuck.

  Conditions: This symptom observed in Cisco IOS Release 15.1T when IP SLA UDP jitter operations are restarted via SNMP.

  Workaround: There is no workaround, except for a router reload.

- 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.

- CSCtf48094

  Symptoms: UUT crashes for FTP traffic with debugs enabled for IPv6 inspection.

  Conditions: The symptom is observed only with Legacy Firewall for IPv6 inspection.

  Workaround: There is no workaround.

- CSCtf48179

  Symptoms: When using an authentication header only (no encryption over the tunnel), a percentage of the outgoing traffic is dropped by the receiver due to incorrect IP header checksums. The percentage dropped depends on the traffic that is flowing over the tunnel.

  Conditions: This problem occurs only when the traffic mix over the tunnel includes both packets with the DF bit set and packets with the DF bit clear. When the DF bit setting differs between two subsequent packets, the second packet is sent with an incorrect IP header checksum.

  Workaround: There is no workaround.

- CSCtf70365

  Symptoms: When “config ED” is used for EEM with some special configurations (like virtual-template commands), it can trigger error messages.

  Conditions: The symptom is observed only when certain commands are configured.

  Workaround: Use “syslog ED”.

- 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.

- CSCtf78196

  Symptoms: Although tunnel interface has alternative path to an OSPF neighbor, when the primary interface goes down, the tunnel interface goes down for a moment.

  Conditions: The symptom occurs when a tunnel tracks an MTU from higher value to a lower value on the outgoing interface.

  Workaround: Statically configure “ipv6 mtu <mtu>” on tunnel interfaces.

- CSCtf79264

  Symptoms: A Cisco route processor (RP) loses part of its odr-route for the spoke network. With a busy network, and with more than 1000 spokes, the second RP can have the same symptom.

  Conditions: This symptom is observed with a default odr timer.

  Workaround: Modifying the odr timer can help, but will not solve the problem.

- CSCtf84393

  Symptoms: A Cisco gateway is unable to place outbound calls from the BRI port when the MGCP gateway is in SRST mode. The call disconnects with cause value = 63 (service/option not available).

  Conditions: This symptom is observed in Cisco IOS Release 12.4(20)T4, Release 12.4(24)T2, and Release 15.0(1).

  Workaround: There is no workaround.

- CSCtf98087

  Symptoms: A Cisco router reloads at sipSPIUpdSrtpSession.

  Conditions: This symptom is observed after completion of the basic call with a hold/resume scenario with IPv6 mode.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCtg25798

  Symptoms: The issue is associated with the two labels imposition for the next-hop address. If there is no label bind for the destination prefix and in order to reach next-hop address the router imposes two labels, only one label is imposed for the final prefix.

  Conditions: The symptom occurs when all of the following conditions are met:

  1. The prefix does not have a label bind (BGP prefixes for example).
  2. There is a static route for the next-hop address pointing to the tunnel only.
  3. The router imposes two labels for the next-hop address.

  Workaround: There are three potential workarounds:

  1. Explicit next hop avoiding recursive research: “ip route 192.168.4.4 255.255.255.255 Tu1 192.168.4.4" (i.e.: breaking rule 2).
  2. Use “neighbor 192.168.1.1 send-label” on both PEs (i.e.: breaking rule 1).
  3. Use “mpls traffic-eng signaling interpret explicit-null verbatim” on P (i.e.: breaking rule 3).

  Further Problem Description: In the following example 192.168.200.200 is the final destination. There is no label bind for this prefix and it is recursive to 192.168.100.100:

  ```
  PE1#sh mp ld bin 192.168.200.200 32 lib entry: 192.168.200.200/32, rev 35 local
  binding: label: 31

  PE1#sh ip route 192.168.200.200 Routing entry for 192.168.200.200/32 Known via
  “static”, distance 1, metric 0 Routing Descriptor Blocks: * 192.168.100.100 Route
  metric is 0, traffic share count is 1
  ```

The next-hop 192.168.100.100 has a static route pointing to the tunnel and is double tagged:

```
PE1#sh ip route 192.168.100.100 Routing entry for 192.168.100.100/32 Known via
"static", distance 1, metric 0 (connected) Routing Descriptor Blocks: * directly
connected, via Tunnel10 Route metric is 0, traffic share count is 1

PE1#sh ip cef 192.168.100.100 192.168.100.100/32 attached to Tunnel10 label 26

PE1#sh mp ld bin 192.168.100.100 32 lib entry: 192.168.100.100/32, rev 30 local
binding: label: 29 remote binding: lsr: 192.168.2.2:0, label: 26 remote binding: lsr:
192.168.4.4:0, label: 26 <<<<< tunnel head-end
```

So the traffic to 192.168.200.200 should also be double tagged as shown below:

```
PE1#sh ip cef 192.168.200.200 192.168.200.200/32 nexthop 192.168.100.100 Tunnel10
label 26
```

However traffic is leaving the router only with the tunnel label:

```
PE1#trace 192.168.200.200 Type escape sequence to abort. Tracing the route to
192.168.200.200 1 192.168.12.2 [MPLS: Label 20 Exp 0] 4 msec 0 msec 0 msec 2
192.168.23.3 [MPLS: Label 23 Exp 0] 4 msec 0 msec 0 msec 3 192.168.34.4 4 msec 0 msec
0 msec 4 192.168.48.8 4 msec * 4 msec
```

- CSCtg30795

  Symptoms: Calls are not torn down since SIP INFO with Qsig disconnect tunneled are not honored by the SIP gateway.

  Conditions: This symptom is observed when disconnect is built and sent by Call manager over a Qsig-enabled SIP trunk to the SIP gateway (GW).

  CUCM1----SIP-QSIG-----SIP GW--------T1 QSIG----------MGCPGW--------CUCM2

  In the above setup, when CUCM1 initiates disconnect, it sends out INFO tunneled with Qsig disconnect to the SIP GW in order to achieve 3-way disconnect.

  Workaround: There is no workaround.

  Further Problem Description: The gateway should send a Qsig Disconnect over the T1 link; since that is not happening, the call is not torn down.

- CSCtg31434

  Symptoms: A Cisco router crashes due to an unexpected exception to the CPU.

  Conditions: This symptom occurs when the **privilege interface level 10 ppp authentication** command is entered. This symptom is observed in Cisco IOS Release 12.2(31)SB through Release 12.2(31)SB18, and in Cisco IOS Release 12.2(33)SB and Release 12.2(34)SB.

  Workaround: There is no workaround.

- CSCtg32567

  Symptoms: IPv6 global addresses are not installed on a DHCP PD client interface.

  Conditions: This symptom is observed when a DHCP client is configured for prefix delegation as well as defined to get an IPv6 address through the prefix delegation. The prefix is obtained from the DHCP server as expected, but the global address is not assigned to the client interface.

  Workaround: There is no workaround.

- CSCtg35257

  Symptoms: The message “previous instance of CNS Event Agent still executing” is seen even if a CNS event is not configured.

  Conditions: The symptom is observed if the **cns event <IP> encrypt** command is enabled and disabled.

  Workaround: There is no workaround.

- CSCtg35298

  Symptoms: Traffic drops are seen between two PEs after re-optimization.

  Conditions: The symptom is observed with 16k VPLS VC, 4k scalable EoMPLS, 1K software EoMPLS, 600 primary tunnels to nPE1 and one tunnel to nPE2 from nPE3.

  Workaround: There is no workaround.

- CSCtg41733

  Symptoms: Certain crafted packets may cause a memory leak in the device in very rare circumstances.

  Conditions: This symptom is observed on a Cisco IOS router configured for SIP processing.

  Workaround: Disable SIP if it is not needed.

- CSCtg42279

  Symptoms: A Cisco label switch router (LSR) crashes when an MPLS traceroute is issued.

  Conditions: This symptom is observed when executing MPLS traceroute over a IPsec-protected GRE tunnel.

  Workaround: There is no workaround.

- CSCtg44108

  Symptoms: Bus error crashes occur frequently.

  Conditions: This symptom is observed on a Cisco 3945e Integrated Services Router (ISR) running Cisco IOS Release 15.1(1)T. IPSec is configured on a GRE multipoint tunnel interface.

  Workaround: There is no workaround.

- CSCtg47129

  Symptoms: A memory leak is seen when NAT is configured.

  Conditions: This symptom is observed when NAT is configured.

  Workaround: There is no workaround.

- CSCtg49109

  Symptom: After a switchover, some of the modules go to MajFail state.

  Conditions: This issue is observed when high traffic is triggered, a lot of packets are dropped by the platform, and numerous IPC messages time out.

  Workaround: There is no workaround.

  Further Problem Description: Due to some unexpected events, one of the IPCs boolean “IPC message blocked” is failing to get set (that is, failing to get unblocked), which is in turn blocking the ICC process from processing further messages. This results in the failure.

- 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.

- CSCtg52885

  Symptoms: The HSRP state on dot1q sub-interfaces remain in INIT state.

  Conditions: This symptom is observed after a physical link flap on a trunk port.

Workaround: Perform a shut/noshut on the interface.

- CSCtg53953

  Symptoms: A standby router reloads due to a parser sync issue when applying certain neighbor commands (**neighbor** <*ip-address*> **disable-connected-check**, **neighbor** <*ip-address*> **peer-group pgrp**, and others).

  Conditions: This symptom applies only to situations where <*ip-address*> is the IP address of a peer that has a dynamically created session (a neighborship that is the result of the "bgp listen range..." feature).

  Workaround: There is no workaround. Such a configuration should not be applied in the first place.

- CSCtg56013

  Symptoms: Router crashes when initiating ping through the modem after router bootup.

  Conditions: The symptom is observed when the modem fails to enumerate at bootup.

  Workaround: There is no workaround.

- CSCtg58786

  Symptoms: When an external interface on the BR is shut down, the BR could be crashed.

  Conditions: If more than one thousand Application Traffic Classes are configured on MC, and if that traffic is traversing through an external interface on a BR, and if the external interface is shut down, this could result in a crash.

  Workaround: There is no workaround.

- CSCtg59158

  Symptoms: A Cisco router console is flooded with the following error messages:

  ```
  crypto_engine_ps_vec: DF_BIT_STATUS_OK Check failed crypto_engine_ps_vec:
  DF_BIT_STATUS_OK Check failed
  ```

  Conditions: This symptom is observed when new SAs are installed during rekeys or after clearing existing SAs. This symptom is observed when GETVPN (crypto map) is configured along with WAAS.

  Workaround: Cryptomaps are not supported in the current phase of WAAS- Express. Please use VTI or unconfigure WAAS-Express.

- CSCtg59328

  Symptoms: When IPCP renegotiates for an existing PPPoE session, the new IPv4 address does not get synced up with the standby.

  Conditions: This symptom is observed when the following tasks are completed:

  - Bring up a PPPoE session and ensure that it is synced to standby.
  - From the PPPoE client run the commands **no ip address** followed by **ip address negotiated** under the Virtual- template interface.
  - As part of the **no ip address** command, the session would first go down on both active and standby. The **ip address negotiated** command would then trigger IPCP re-negotiation and the session would come up on active. On standby, the session remains down and the new IP address is not synced.

  Workaround: There is no workaround.

- CSCtg59956

  Symptoms: Active supervisor crashes when doing an SSO switchover.

Conditions: The symptom is observed when performing a switchover operation with a lot of L2VPN NLRIs. BGP L2VPN configuration is required.

Workaround: There is no workaround.

- CSCtg60201

  Symptoms: Unconfiguring the **maximum-path** command does not trigger a backup path calculation.

  Conditions: This symptom is observed if addition-path install is configured along with the **maximum-path** command.

  Workaround: Reconfigure “bgp additional-path install.”

- CSCtg60302

  Symptoms: CPP ucode crashes after shutting down mpls-te tunnel interfaces.

  ```
  ixia ------PE1 ------------PE2 --------------ixia
  ```

  This is a 6PE topology with an MPLS TE tunnel between PE1 and PE2 and traffic passing through the TE tunnel. When the TE is shut down, the CPP crashes.

  Conditions: This symptom is observed when the traffic rate is about 500 packets per second.

  Workaround: There is no workaround.

- CSCtg68012

  Symptoms: The following logs are created by the Cisco 6509 switch:

  ```
  Apr 29 10:21:17.335 BST: %SCHED-3-THRASHING: Process thrashing on watched message
  event. -Process= “RTTYS Process”, ipl= 5, pid= 78 -Traceback= 410545B0 41054694
  418628A8 Apr 29 10:22:57.379 BST: %SCHED-3-THRASHING: Process thrashing on watched
  message event. -Process= “RTTYS Process”, ipl= 5, pid= 78 -Traceback= 410545B0
  41054694 418628A8 Apr 29 10:24:37.427 BST: %SCHED-3-THRASHING: Process thrashing on
  watched message event. -Process= “RTTYS Process”, ipl= 5, pid= 78 -Traceback= 410545B0
  41054694 418628A8
  ```

  Conditions: This symptom is observed on a Cisco 6509 switch running Cisco IOS Release 12.2(18)SFX6.

  Workaround: There is no workaround.

- 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.

- CSCtg76688

  Symptoms: An active Cisco route processor reloads in a scale scenario (16k - 24k sessions) when the **clear subscriber session all** command is entered.

  Conditions: This symptom is observed only when there are 16k-24k sessions and the **clear subscriber session all** command is entered.

  Workaround: Do not enter the **clear subscriber session all** command when more than 16k sessions are up on the router.

- CSCtg83932

  Symptoms: “Encapsulation aal5auto” may not be enabled under svc mode.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(01.14)T.

  Workaround: There is no workaround.

- CSCtg84649

  Symptoms: EIGRP is not forming adjacencies over virtual interfaces in a DVTI environment.

  Conditions: This symptom is observed on a Cisco ASR 1000 platform with Cisco IOS Release 12.2(33)XNE or Release 12.2(33)XNF1.

  Workaround: Remove the passive-interface configurations for Virtual-Template and then re-configure the passive-interface designation. For example,

  ```
  Router#sh run | b router router eigrp 100 network 10.1.0.0 0.0.31.255
  passive-interface default no passive-interface Virtual-Template1
  ```

  ```
  Router(config)#router eigrp 100 Router(config-router)#no passive-interface default
  Router(config-router)#passive-interface default Router(config-router)#no passive
  Virtual-Template 1
  ```

- CSCtg86714

  Symptoms: The **show cellular 0** command might not show any output.

  Conditions: The symptom is observed with the **show cellular 0** command.

  Workaround: Shut down the cellular 0 interface, write the configuration to memory and reboot, so that the configured interface is shutdown on boot. You then have your original start up configuration, with the cellular 0 shut down, and you still get **show cellular stats**. If you then unshut the cellular after the “MODEM UP” line, you get “LINK UP” and still retain the **show cellular stats**.

- CSCtg87775

  Symptoms: The router may unexpectedly reload.

  Conditions: The symptom is observed under circumstances where a Cisco 7600 series router is configured to handle several hundred or more neighbors, and an administrator issues the command: **clear bgp vpnv4 unicast ***.

  Workaround: Clear individual neighbors separately, limiting yourself to 100 or fewer in any scanner interval.

Further Problem Description: Issuing other clear commands and forcing a switchover between active and standby at during the interval immediately before and after issuing the BGP clear command increases the probability of a reload.

The number of neighbors where this is documented as happening is 1200, but the exact minimum number of neighbors needed to trigger the problem is not documented.

- CSCtg88766

  Symptoms: HWIC-SHDSL does not train up in 4-wire standard mode.

  Conditions: The symptom is observed when CPE is in 4-wire standard mode and the DSLAM linecard is GSPN-based and configured in 4-wire standard mode.

  Workaround: There is no workaround.

- CSCtg91201

  Symptoms: DHCP-added static routes get removed sometimes and the traffic towards the host gets dropped.

  Conditions: The symptom is observed with IP unnumbered relay and with a third party external DHCP server. (This issue can also occur with an IOS DHCP server, but the probability is quite low.)

  Workaround: There is no workaround.

- CSCtg91336

  Symptoms: A Cisco router may crash during show command **show ip ospf rib** execution.

  Conditions: This symptom is observed in Cisco IOS releases with enhancement CSCsu29410 when the following sequence of events occurs:

  – A user enters the **show ip ospf rib** command and stops in the middle.

  – The OSPF local rib is significantly changed; for example, routes are removed.

  – A user presses Enter or spacebar to resume output of the **show ip ospf rib** command.

  Workaround: Do not enter the **show ip ospf rib** command. If it is necessary to use the command, enter **terminal length 0** and print the entire output.

- CSCtg92783

  Symptoms: Uplink performance degrades by about 70% with HWIC-3G-CDMA when bound to external dialer interface when compared to using cellular interface legacy DDR.

  Conditions: This symptom is seen on live network when performance is measured using latency sensitive Internet speed test application.

  Workaround: Use cellular interface without binding to external dialer.

- CSCtg94250

  Symptoms: Removing **address-family ipv4 vrf <vrf>** (in router BGP) followed by **no ip vrf <vrf>** (where “vrf” is the same) could result in a crash.

  Conditions: The symptom is observed in a large VPNv4 scale setup, when applying the following commands to the same VRF back-to-back:

  1. **no address-family ipv4 vrf <vrf>**
  2. **no ip vrf <vrf>**
  3. **ip vrf <vrf>**

  The trigger of the BGP crash is a result of a racing condition between event 1 and event 2.

Workaround: Since this is a racing condition, the workarounds are:

1. Not applying (1) before (2).
2. Give sufficient time for (1) to complete before applying (2).

- CSCtg95618

  Symptoms: 1. MSCD_StartStop fail message is observed in usbflash_mscd_scsi_listener 2. USB flash file system is not accessible sometimes.

  Conditions: This symptom is observed on Cisco 892F and C892FW series routers with two USB slots when the USB sticks are removed and swapped. This symptom is not observed when a single USB stick is removed or inserted in a different bus.

  Workaround: There is no workaround.

- CSCtg95940

  Symptoms: The DH operation will fail and no further IKEv2 SAs will come up.

  Conditions: This issue can occur with many IKEv2 requests coming at once and when you are using hardware crypto-engine.

  Workaround: There is no workaround.

  Further Problem Description: You can re-start the router and switch to software-crypto engine if needed.

- CSCtg96518

  Symptoms: Fast memory leak occurs in CCSIP CCB Pool.

  Conditions: This symptom is observed on a Cisco 2951 integrated services router with Cisco IOS Release 15.1(1)T.

  Workaround: Reload the router.

- CSCtg96630

  Symptoms: A Cisco router crashes when the user tries to configure a default policy with rsvp group percentage configuration.

  Conditions: This symptom is observed when the user tries to configure a default policy with rsvp group percentage configuration under a virtual template.

  Workaround: There is no workaround except to avoid this configuration command.

- CSCtg98783

  Symptoms: Cube: call leg 1 receives SDP 101, 0-15; Cube: call leg 2 sends SDP 101, 0-16. This is seen as a different media, and is treated as such.

  Conditions: This symptom is observed when Cube is configured in DO-EO with flow-around.

  Workaround: There is no workaround.

- CSCtg99114

  Symptoms: The following error message with traceback is observed:

  ```
  %IPC-5-REGPORTFAIL: Registering Control Port
  ```

  Conditions: The symptom is observed with ISR routers and with Cisco IOS Release 12.4(24)T or later.

  Workaround: Drop IPC traffic using control-plane policing:

  ```
  class-map match-all ipc match access-group name ipc policy-map drop-ipc class ipc drop
  ip access-list extended ipc permit udp any any eq 1975 control-plane service-policy
  input drop-ipc
  ```

- CSCth01394

  Symptoms: On a Cisco 7606 router that is running Cisco IOS Release 12.2(33) SRD3 with SIP200/SPA-4XCT3/DS0, when you have ppp multilink interface(s) configured with member links from same SPA (software based multilink) and you physically remove SPA, you will see that upon executing the **show ppp multilink** command, the multilink interface still has reference for member links. If you do the **sh run int serialx/y** command, you will get message interface not found.

  Conditions: This issue is consistently reproducible.

  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.

- CSCth02725

  Symptoms: There is an interoperability issue between a third-party vendor's routers and Cisco routers with severe IPTV service failure in Prune-Overriding environment.

  Conditions: The symptom is observed in the following scenario:

  1. Router A is Cisco 7609 router (IP address 10.1.1.1) and connects to Router B (third-party vendor's router; IP address 10.1.1.3) and Router C (IP address 10.1.1.2).
  2. If subscriber under Router C disappears, Router A receives "Prune" message from Router C.
  3. Router A does not change "source IP of PruneEcho message (10.1.1.2)" and sends it to Router B.
  4. At this time, Router B should send overriding-join to Router A because Router B still has subscribers. But Router B drops the PruneEcho message because source IP (10.1.1.2) is not from PIM neighbor. Router B cannot send overriding-join to Router A. 5. As a result, multicast traffic (IPTV stream) to Router B stops.

  Workaround: Connect C and B to become PIM neighbors. However, this cannot always be considered a recommended workaround because of potential high cost and/or other (sometimes third-party) limitations.

- CSCth02789

  Symptoms: System can crash when attempting to schedule an IPv6 icmp-echo operation.

  Conditions: The symptom is observed with IPv6 and icmp-echo.

  Workaround: There is no workaround.

- 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.

- CSCth03379

  Symptoms: A Cisco router reloads while booting with DSL configurations.

  Conditions: This symptom is observed on a Cisco router with Cisco IOS Release 15.1(1.15)T configured with DSL controller.

  Workaround: There is no workaround.

- 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.

- CSCth04945

  Symptoms: A Cisco router crashes when adding or removing a QoS policy from an interface.

  Conditions: This symptom is observed when the following occur:

  - packets keep hitting the interface from which the policy is being removed
  - the QoS policy is at least a two-level policy
  - before the policy was removed, the CLI generated an error for some invalid configuration change in that policy; for example,

  ```
  3845-AA2205(config)#policy-map VOICE-OUT-PARENT 3845-AA2205(config-pmap)#class
  class-default 3845-AA2205(config-pmap-c)#no shape average 100000000 Queueing must be
  removed from child classes before queueing can be removed from class-default
  ```

  Workaround: Avoid invalid configuration changes in the QoS policy before adding it to or removing it from an interface.

- CSCth05778

  Symptoms: Router is showing memory leaks.

  Conditions: The symptom is observed when the remote end is sending LCP conf_req messages to a Cisco 10000 series router more frequently (1 per 4 msec) than the normal scenario (1 per 2 seconds).

  Workaround: Shut down the PPP link that is flapping.

- CSCth06812

  Symptoms: A Cisco ASR 1000 sees a hang followed by a crash.

  Conditions: This symptom is observed on a Cisco ASR 1000 with Cisco IOS Release 2.5.1. (XNE1) and the following configuration:

  ```
  R1(config)#parser view SUPPORT R1(config-view)# secret cisco R1(config-view)#
  commands exec include ping R1(config-view)# commands exec include configure terminal
  R1(config-view)# commands exec include show ip ospf neighbor <--Where we see the hang
  ```

  Workaround: Do not configure **commands exec include show ip ospf neighbor** command in parser view configuration.

- CSCth07787

  Symptoms: A standby device crashes when attempting to configure login banner on the active device.

Conditions: The symptom is observed only when configuring the banner manually, but not during bulk sync or any copy operations. In addition, this symptom is observed when using the following delimiters: -Cntrl-v + Cntrl-C -Shift-6 + Shift-C

Workaround: Use any delimiters other than the following: -Cntrl-v + Cntrl-C -Shift-6 + Shift-C

- CSCth08505

  Symptoms: PPPoE sessions may not sync to the standby-RP.

  Conditions: This symptom is observed after the first attempt at establishing a PPPoE session fails.

  Workaround: Reloading the standby-RP may resolve this issue.

- CSCth09876

  Symptoms: Cisco IOS IP Service Level Agreements (SLAs) cannot be auto-discovered if IP SLAs are removed from the responder first.

  Conditions: This symptom is observed on a Cisco device after IP SLAs have been unconfigured. Subsequent attempts to reconfigure the device as an IP SLAs responder fail.

  Workaround: Reload the router and configure the device as an IP SLAs responder.

- CSCth10764

  Symptoms: PPP Negotiation not working correctly between Cisco GSR XR and Cisco 7200.

  Conditions: Max-header size different on both ends, PPP not negotiating lower size.

  Workaround: There is no workaround.

- CSCth11747

  Symptoms: When a switchover occurs with GR enabled, sometimes the NSF states are not preserved and the forwarding entries are lost, leading to packet loss for a few seconds.

  Conditions: This symptom is observed only with single sessions with GR configured when the restarting neighbor does a passive open. Chances of hitting this are low since this issue occurs because we receive a new open message before the old tcp session has a chance to reset.

  Workaround: Configuring multi-session capability on the neighbor sessions or restricting the restarting neighbors connection to active mode would prevent this issue.

  Further Problem Description: When an established session already exists between the GR-enabled routers, and the tcp has not yet notified of reset due to neighbor SSO, if the receiving router gets a new open from the restarting router, as per the RFC it is supposed to tear down the old session and accept the new connection. The old session was being torn down properly but it would take the service reset walker to completely free the session. In case of multi-sessions there was no problem in accepting the new session since multiple sessions are allowed. But in case of a single session that already exists, the new sessions are not allowed until the old session is completely freed. Hence, the new session was getting rejected and notification was sent to the restarting neighbor. The restarting neighbor, upon reception of this notification, would clear the NSF preserve bits and further opens would clear the NSF states on the receiving neighbor and hence the problem. The solution would be to accept the new connections in single session support neighbors when the GR reopen has marked the session for reset and de-linked the topologies. The topologies would be added to the new session and the connection accepted. The old session would be freed when service reset walker is invoked. So, for a transient period of time between the session mark reset and the session free, there would be multiple sessions established on the neighbor even though the neighbor was configured as single session. Dependent DDTS CSCtd99802 and CSCth90239 need to be committed along with this fix to ensure complete working of this functionality.

- CSCth13153

  Symptoms: An incorrect UDLR Reporter exists on a router that is connected to a UDLR link and PIM-SM domain with auto-rp configurable.

  Conditions: This symptom is observed on a Cisco 7200 series router with Cisco IOS Release 15.1(1.16)T0.1.

  Workaround: There is no workaround.

- CSCth15105

  Symptoms: BFD sessions flap after unplanned SSO (test crash).

  Conditions: The symptom is observed on a UUT up with unicast/multicast along with BGP and BFD configurations. For BFD timers of 1*5, 500*8, after doing a test crash (option C followed by 6), we see BFD sessions flap.

  Workaround: There is no workaround.

- 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.

- CSCth15353

  Symptoms: Incorrect result codes are displayed in vpdn sys logging. The CDN message for admin down was reported in the syslog as “Result Code=2, Error Code=6” instead of “Result Code=3, Error Code=6”.

  Conditions: This symptom is observed when a session is cleared by a clear command (for example, **clear interface virtual-access 3.1**).

  Workaround: There is no workaround.

- CSCth15518

  Symptoms: Ping through ISDN BRI interface fails.

  Conditions: The symptom is observed when attempting a ping after giving a **shut** and **no shut** on the BRI interface.

  Workaround: There is no workaround.

- CSCth15519

  Symptoms: A Cisco router reloads with “show memory <invalid-address_value>”.

  Conditions: This symptom is observed on Cisco 1861, 880, and 860 routers.

  Workaround: There is no workaround.

- CSCth16011

  Symptoms: After a network event is introduced in the network, such as a 3- percent loss, MOS policy will detect the OOP condition. But PfR will let the prefix stay in the OOP condition for some time and then switch over to an alternative exit.

  Conditions: Introduce loss to network.

  Workaround: There is no workaround.

- 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.

- CSCth18611

  Symptoms: A Cisco router crashes.

  Conditions: This symptom is observed when configuring dynamic nat under the vrf interface with an existing firewall configuration. This symptom is not observed without the vrf configuration.

  Workaround: There is no workaround.

- CSCth18982

  Symptoms: BGP sessions flap continuously in a multi-session configuration.

  Conditions: This symptom is observed when the same peer under the same address family is configured under different topologies (MTR with GR-enabled setup) with multiple topo-ids.

  Workaround: The sessions do not flap if topologies use the same topo-id (tid) for the peers active under different topologies or when GR is not enabled.

- CSCth20704

  Symptoms: A Cisco router crashes when policy-map is unconfigured while traffic is flowing.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(1)T1.

  Workaround: There is no workaround.

- CSCth21017

  Symptoms: Traceback is seen when ISIS adjacency state changes.

  Conditions: This symptom is observed on a Cisco 7200 router running Cisco IOS Release 15.1(1)T1.

  Workaround: There is no workaround.

- CSCth23787

  Symptom: A Cisco router crashes at “mcast_aaa_send_stop_acct_event.”

  Conditions: This symptom is observed while unconfiguring “ipv6 mld join-group FF1E:7777:7777::1” in the client after configuring within 15-20 seconds.

  Workaround: Unconfigure, if required, after multicast start record is sent.

- CSCth23814

  Symptoms: When using Flexible NetFlow, a traceback or crash can occur.

  Conditions: This symptom is observed when a monitor is configured with a flow record that has the “BGP next hop” field configured.

  Workaround: Ensure that the “BGP next hop” field is not configured for a flow.

- CSCth25634

  Symptoms: The password is prompted for twice for authentication that is falling over to the line password.

  Conditions: This symptom is observed when login authentication has the line password as fallback and RADIUS as primary. For example:

  ```
  aaa authentication login default group radius line
  ```

  Workaround: Change the login authentication to fall back to the enable password that is configured on the UUT. For example:

  ```
  enable password <keyword> aaa authentication login default group radius enable
  ```

- CSCth25698

  Symptoms: IPv6 packets are not dropped by the firewall.

  Conditions: IPv6 packets are not dropped by the firewall in case of Zone to non-zone.

  Workaround: There is no workaround.

- CSCth26441

  Symptoms: Non-broadcast Ethernet frames are dropped by the Gig1/0 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.

- CSCth28677

  Symptoms: CUD fails to be parsed when it contains 0x00.

  Conditions: This symptom is observed on a Cisco router configured for X25 translation with CUD verification.

  Workaround: There is no workaround.

- CSCth30815

  Symptoms: StopCCN result codes and strings do not match RFC.

  Conditions: This symptom is observed when the session is cleared by command or due to some error condition; the result code is not correct.

  Workaround: There is no workaround.

- CSCth31271

  Symptoms: A Cisco ASR router crashes with next-hop recursive.

  Conditions: This symptom is observed after the following tasks are executed:

  1. Configure a route-map with recursive next-hop clause for ip address (for example, 1.2.3.4)
  2. Change the recursive next-hop to ip address (for example, 5.6.7.8)
  3. Apply PBR with this route-map to an interface
  4. Delete the route-map
  5. Shut the interface.

  Workaround: There is no workaround.

- CSCth31395

  Symptoms: Frame-relay PVC stays in INACTIVE state.

Conditions: The symptom is observed with Cisco IOS interim Release 15.0(1) M2.14.

Workaround: There is no workaround.

- CSCth33457

  Symptoms: A Cisco IOS router configured with IPSec 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.

- CSCth33804

  Symptoms: Traffic is dropped at CPP with error message “noipv4route” after RP switchover, and traffic on few sessions is dropped.

  Conditions: This symptom occurs when VRF is configured for PPPoE sessions and RP switchover is done with traffic flowing.

  Workaround: Do not configure VRF.

- CSCth33949

  Symptoms: An LNS standby crashes when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the command **clear ppp all**.

  Conditions: This symptom is observed when 1000 IPv6 PPPoEoA sessions are cleared from LNS using the command **clear ppp all.**

  Workaround: Use the **cle vpdn tunnel l2tp all** command instead.

- CSCth35377

  Symptoms: Master router does not reacquire DLSW Circuits after failing over to slave router and back again.

  Conditions: This symptom is observed on a GigabitEthernet interface on a Cisco 2921 master router running DLSW ethernet redundancy and with the following parameters: encapsulation dot1Q xxx ip pim sparse-mode.

  Workaround: Remove “ip pim sparse-mode.”

- CSCth35620

  Symptoms: Self zone inspection fails for TCP/UDP and ICMP traffic.

  Conditions: The symptom is observed when the interface is part of self zone and router-terminated traffic hits that interface.

Workaround: There is no workaround.

- CSCth35780

  Symptoms: A Cisco router crashes for the SIP multi-part traffic.

  Conditions: This symptom is observed when SIP multi-part traffic passes through a Cisco 7200 router. NAT SIP Multi-part must be enabled as part of the NAT configuration.

  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.

- CSCth36740

  Symptoms: A router may experience CRC and Runt errors.

  Conditions: The symptom is observed with Cisco IOS Release 15.0(1)M2 and when the onboard GigabitEthernet interface is hard-coded to 10mb/full duplex. It is seen with the following routers: Cisco 1900 series, Cisco 2900 series, and Cisco 3900 series.

  Workaround: There is no workaround.

- 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.

- CSCth38711

  Symptoms: The first WAAS connection takes longer than one minute to begin transferring data.

  Conditions: This symptom is observed during AOIM sync, which occurs once per boot or reconfiguration.

  Workaround: There is no workaround.

- CSCth39774

  Symptoms: UUT hangs when an eTCDF file is loaded on the router in the latest t_base_1 code base.

  Conditions: The symptom is observed when an eTCDF file is loaded on the router, the UUT seems to hang. However, the UUT is actually waiting for user input, and if you enter "#" on the CLI, it will print some error messages about invalid commands and return to CLI.

  Workaround: Do not use the eTCDF file to configure the encrypted filter, rather directly enter the commands on the CLI of the router.

- CSCth39877

  Symptoms: No VPDN logging occurs for the L2TP tunnel.

  Conditions: This symptom is observed when the tunnel goes down.

Workaround: There is no workaround.

- CSCth40090

  Symptoms: A Cisco device crashes when initiating an analog CAMA call.

  Conditions: On initiation of an analog CAMA call, a crash occurs due to memory corruption leading to a breakpoint exception. A crash occurs in scenarios where e911 is enabled or disabled.

  Workaround: There is no workaround.

- CSCth40213

  Symptom: More than one preshared key for address 0.0.0.0 may not be configurable in different keyrings.

  Conditions: Multiple preshared keys cannot be configured for address 0.0.0.0 in different keyrings.

  Workaround: There is no workaround.

- CSCth40506

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

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

  Workaround: There is no workaround.

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

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

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

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

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

- CSCth42594

  Symptoms: Remote standby router crashes when you configure and remove “ppp multilink mrru local” under a multilink interface.

  Conditions: The symptom is observed with the following conditions:

  - When multilink is bundled with more than one serial interfaces (not seeing this issue with only one serial interface).
  - Seeing this issue from 1500 and above (not seeing this issue when configure and remove “ppp multilink mrru local 1499").

  Workaround: There is no workaround.

- CSCth42798

  Symptoms: In a very corner case, when BGP is in read-only mode and attributes are deleted before the networks, memory can be corrupted.

  Conditions: The device should be in read-only mode, and attributes should be deleted before networks.

  Workaround: There is no workaround.

- CSCth42999

  Symptoms: Serial HWICs (HWIC-4T/4AS/8AS/4A/16A) are not functional after the commit of CSCth18756 (FPGA firmware compressed within IOS image).

Conditions: The symptom is observed when you plug the serial HWIC into the eHWIC slot of the router and test the ping for that particular serial interface.

Workaround: There is no workaround.

- CSCth45623

  Symptoms: A memory leak occurs in cce dp reclass.

  Conditions: This symptom is observed with WAAS Express plus QoS preclassify disabled plus Crypto plus crypto-map.

  Workaround: There is no workaround.

- CSCth45731

  Symptoms: PPPoE sessions get synced partially to the standby RP and later never get cleaned up. The **show** command for the sessions looks on a standby RP like the following:

```
Sby#show ppp all Interface/ID OPEN+ Nego* Fail- Stage Peer Address Peer Name
------------ -------------------- -------- --------------- ------------------ --
0xB400008A LCP+ CHAP+ IPV6CP+ Undefine 0.0.0.0
```

  Peer address is 0 and interface will show the PPP handle instead of the virtual interface of PPP.

  Conditions: This symptom is seen when IPCP is getting renegotiated and terminated before the full session sync is done for the upcoming PPPoE session.

  Workaround: There is no workaround.

- CSCth46540

  Symptoms: Configuring **memory-size iomem** returns an error:

```
Maximum IO percent supported for 2560MB memory is 0 (0MB)
```

  Conditions: The symptom is observed on a Cisco 1941 installed with 2.5 GB of DRAM.

  Workaround: There is no workaround.

- CSCth46888

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

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

  Workaround: There is no workaround.

- CSCth47765

  Symptoms: Once a router boots up, FXS/FXO voice-port in slot2 stays in “S_OPEN_PEND” state. The DSP from the MB that provides resources to the EVM-HD-8FXS/DID and EM-HDA-3FXS/4FXO cards in slot 2 goes into “FW_DNLD_FINISHED” state which causes the voice ports on EVM-HD-8FXS/DID and EM-HDA-3FXS/4FXO cards to go into “S_OPEN_PEND state”.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.1(1) T0.9 with 26.8.0 DSPware.

  Workaround: There is no workaround.

- CSCth48009

  Symptoms: Changes to IOS-WAAS syslog messages.

  Conditions: The symptom is observed with syslog messages for IOS-WAAS.

Workaround: There is no workaround.

- 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.

- CSCth49421

  Symptoms: Transparent bridging stops working.

  Conditions: The symptom is observed when the interface goes to standby from active. The output of **show controllers gigabitethernet** *slot/port* shows these fields (at the end of output):

  When working:

  Software filtered frames: 0 Unicast overflow mode: 1 <-- Multicast overflow mode: 1 Promiscuous mode: 1 Total Number of CAM entries: 8 Port Stopped: N

  When not working:

  Software filtered frames: 0 Unicast overflow mode: 0 <-- Multicast overflow mode: 1 Promiscuous mode: 1 Total Number of CAM entries: 4 Port Stopped: N

  Workaround: Remove bridging and reconfigure it on the interface.

- CSCth50479

  Symptoms: With high rate of session churn, the **show subscriber sessions** command shows sessions are stuck in the “Attempting” state. The **show subscriber stat detail** command shows that these sessions are actually stuck in the “installing-config” state.

  Conditions: The symptom is observed with a high rate of PPP session churn and with a large number of sessions (resulting in more than 70% IOS memory used).

  Workaround: Router reload is required to clear stuck sessions.

- CSCth50550

  Symptoms: A Cisco device crashes when using PDP filter.

  Conditions: This symptom is observed when PDP filter is applied in a QoS Policy.

  Workaround: There is no workaround.

- CSCth51125

  Symptoms: PCEX-3G-HSPA-R6 is not recognized at bootup:

  ```
  %CISCO800-2-MODEM_NOT_RECOGNIZED: Cellular0 modem not RECOGNIZED. Carrier id not
  available or invalid! Replace it with Cisco supported modem and reload the router.
  %CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
  %CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
  %CELL_MSG-1-MODEM_ACK_FAIL: [Cellular0] Modem Ack not received.
  ```

  Conditions: The symptom is observed on a Cisco 881G-K9 that is running Cisco IOS Release 15.1(1)T.

  Workaround: There is no workaround.

- CSCth52485

  Symptoms: A call from the PSTN reaches an AC agent via the AC Route Point and the call is successfully answered. The AC agent then attempts a blind transfer using the AC to another IP Phone, but after around eight seconds of silence the call is dropped.

  On the CUBE we see the following (the below messages exclude the communication between the CUCM and the CUBE as it is irrelevant):

  ```
  -Invite outbound to the PGW -200 OK inbound from the PGW -ACK outbound to the PGW
  -UPDATE outbound to the PGW -200 OK inbound from the PGW -Invite outbound to the PGW
  -200 OK inbound from the PGW -ACK outbound to the PGW -Invite outbound to the PGW -491
  Request Pending inbound from the PGW -ACK outbound to the PGW
  ```

  Then the CUBE receives a BYE after 8 seconds from the CUCM and forwards this to the PGW and the call terminates. After receiving the 491 Request Pending, the CUBE is not forwarding this to the CUCM, whereas all previous SIP messages are forwarded successfully. The CUBE should forward this 491 to the CUCM and then the CUCM should react by sending the Invite again for which it received the 491 Request Pending.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T.

  Workaround: There is no workaround.

- 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 Release 12.4(24)T3, Release 12.4(11)XJ, and Release 15.1(1)T.

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

- CSCth55579

  Symptoms: Router reloads at clean_out_RA_certs after enrolment with CA server.

  Conditions: The symptom is observed after enrollment with CA server.

  Workaround: There is no workaround.

- CSCth57478

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

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

  Workaround: There is no workaround.

- CSCth57542

  Symptoms: The command **show voice dsp command history 1/1:0** reloads a Cisco AS5400XM router if the T1 controller is seated in slot1.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(2)T.

  Workaround: Apply the **show voice dsp command history** command only for the slots having PVDM2 [C5510] DSPs.

- CSCth58283

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

  Conditions: NAT is enabled.

  Workaround: There is no workaround.

- CSCth59123

  Symptoms: QoS policy may not match traffic after a reload. All packets match class-default.

  Conditions: The symptom is observed after you reload the router with QoS policy.

  Workaround: Remove and reapply QoS policy.

- CSCth59217

  Symptoms: Firewall sessions are not seen when ZBFW and gatekeeper are configured on the UUT.

  Conditions: The symptom is observed when ZBFW and gatekeeper are configured on the UUT.

  Workaround: There is no workaround.

- CSCth59784

  Symptoms: Process watchdog timeout crashinfo file not written into flash for Cisco 887 router.

  Conditions: The symptom is observed on a Cisco 887 router.

  Workaround: There is no workaround.

- CSCth61759

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

  Conditions: There are a couple of scenarios where this problem was observed.

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

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

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

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

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

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

  Scenario 2:

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

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

  Workaround: There is no workaround.

- CSCth61827

  Symptoms: Invalid memory action followed by traceback when traffic is on.

  Conditions: The symptom is observed on a Cisco 7200 series router that is running Cisco IOS interim Release 15.1(2.5)T.

  Workaround: There is no workaround.

- CSCth62854

  Symptoms: A Cisco router crashes with traceback ospfv3_intfc_ipsec_cmd.

  Conditions: This symptom is observed when the interface is configured with ospfv3, null authentication/encryption, and non-null encryption/authentication.

  Workaround: Remove the ospfv3 area command, then remove the null authentication/encryption.

- CSCth63379

  Symptoms: With two T1 links running ATM with IMA bundling, the proper CEF- attached adjacency for the opposite end of the link does not appear.

  Conditions: This symptom is observed on a Cisco 3800 series device with VWIC- 2MFT-T1.

  Workaround: There is no workaround.

- CSCth64507

  Symptoms: Bulk Sync failure is seen on redundancy force-switchover command when eem policy is configured and only when the policy file is present in active module.

  Conditions: This issue is observed only when the policy file is present in the active and not in the standby module.

  Workaround: Have the policy file present in both the active and the standby.

- CSCth64589

  Symptoms: The memory allocated at bds_create_link_list & udb_create_ds was leaked. The service policy would not be attached on the interface.

  Conditions: This symptom is seen in Cisco routers loaded with Cisco IOS version of Release 15.1(2.5)T. This happens in corner case configurations where the parent class map has only one filter, which is a nested class.

  Workaround: The following configuration can be modified to make things work.

  ```
  class-map c1 class-map c2 match class c1
  policy-map p1 class c2
  ```

  Replace the above configuration as follows:

  ```
  class-map c1
  policy-map p1 class c1
  ```

  The results are the same.

- CSCth65072

  Symptom: A memory leak occurs in the big buffer pool while using the service reflect feature.

  Conditions: This symptom is observed when the service reflection feature is enabled. A packet is generated from service reflection and is blocked by an ACL on the outgoing interface. This will cause the buffer leak.

  Workaround: Remove the ACL on the outgoing interface or permit the packets generated from service reflect on the ACL.

- CSCth66177

  Symptoms: The standby PRE crash triggers an active PRE crash.

  Conditions: The symptom is observed when the standby PRE crashes due to a memory parity error. The standby PRE crash also triggers an active PRE crash due to bus error.

  Workaround: There is no workaround.

- CSCth66251

  Symptoms: You are not able to configure a policy-map for the second time in a Cisco 860 router. An “internal data base error” message is seen.

  Conditions: The symptom is observed when configuring a policy-map for the second time and with a Cisco 860 router.

  Workaround: There is no workaround.

- CSCth67608

  Symptoms: Some groups are missing in the MLD Proxy cache on the Proxy router.

  Conditions: This symptom is observed when ipv6 mld host-proxy is applied with existing multicast routes.

  Workaround: Clear the multicast routes using clear ipv6 pim topology after applying ipv6 mld host-proxy.

- CSCth67788

  Symptoms: sVTI stops forwarding traffic when a local policy is configured on a device.

  Conditions: The symptom has been observed on a router that is running Cisco IOS Release 15.0(1)M1.

  Workaround 1: Do not use a local policy.

  Workaround 2: Configure “no ip route-cache cef” on the tunnel interface.

- CSCth67811

  Symptoms: Acct-Terminate-Cause is set as “nas-error” in Tunnel stop record when admin clear.

  Conditions: This symptom is seen with admin clear tunnel using the **clear vpdn tunnel l2tp all** command.

  Workaround: There is no workaround.

- CSCth69243

  Symptoms: Error messages and tracebacks involving the TCP timer process appear on the console.

  Conditions: This symptom is observed with a large volume of traffic over extended periods of time; the exact trigger is unknown.

  Workaround: There is no workaround.

- CSCth69361

  Symptoms: A Cisco 881 router crashes when verifying energywise endpoint using an Orchestrator Agent.

  Conditions: The symptom is observed when “energywise endpoint” is configured on a Cisco 881 and when Orchestrator Agent is running.

  Workaround: There is no workaround.

- 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.

- CSCth71349

  Symptoms: Some SSS sessions are staying in “attempting” state for a while when using ISG Static Session Creation.

  Conditions: The symptom is observed when using ISG Static Session Creation.

  Workaround: Stop incoming traffic from subscribers and wait until the sessions recover, then re-apply the traffic.

- CSCth72598

  Symptoms: PVC stays inactive after OIR.

  Conditions: The symptom is observed while performing an OIR on a core-facing interface.

  Workaround: Do not do an OIR.

- CSCth74420

  Symptoms: Vtemplate number is not set in virtual access interface before cloning the commands onto the VA.

  Conditions: The symptom is observed with any application that requests a VA to be cloned from a VT.

  Workaround: There is no workaround.

- CSCth77531

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router with hundreds of IPv4 and IPv6 BGP neighbors shows high CPU utilization in the BGP-related processes for several hours (more than 2.5).

  Conditions: The symptom is observed with Cisco IOS Release 12.2(33)XNF. The BGP task process uses the most CPU; also, the number of routemap-cache entries should be very high.

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

  Workaround: Use “no bgp route-map-cache.” This will not cache the route-map cache results, and the issue will not be observed.

- CSCth78630

  Symptoms: Call manager or other SAF clients are not able to learn SAF patterns.

  On the forwarder, “show eigrp service-family external-client” displays multiple expired client registrations. The keepalive timer on the stale registrations is 0, and the “Client API Handle” is “0”, however the File Descriptor is still listed in the table. See the following example:

  ```
  abi-4506#sh eigrp service-family external-client SAF External Clients Client Label
  Client API Handle File Descriptor ABI_SAF_CLIENT1 0 1 ABI_SAF_CLIENT1 0 2
  ABI_SAF_CLIENT1 0 3 ABI_SAF_CLIENT1 0 4 ABI_SAF_CLIENT1 0 5 ABI_SAF_CLIENT1 0 6
  ABI_SAF_CLIENT1 0 7 ABI_SAF_CLIENT1 0 8 ABI_SAF_CLIENT1 0 9 ABI_SAF_CLIENT1 0 10
  ABI_SAF_CLIENT1 0 11 ABI_SAF_CLIENT1 0 12 ABI_SAF_CLIENT1 0 13 ABI_SAF_CLIENT1 0 14
  ABI_SAF_CLIENT1 15 15 ABI_SAF_CLIENT1 16 16 abi-4506#
  ```

  Using the **debug voice saf** command or the **debug eigrp service-family [external-client {client|messages|protocol}]** command shows the following traceback:

  ```
  %SCHED-3-STUCKMTMR: Sleep with expired managed timer 229C03BC, time 0xF2968 (4d20h
  ago). -Process= “SAF-EC FORWARDER”, ipl= 4, pid= 235 -Traceback= 11A14818 11A14E3C
  11130E54 109A0594 10997584
  ```

  Conditions: This symptom occurs when a SAF client unregisters/re-registers to a SAF forwarder.

  Workaround: Reload the router acting as forwarder and ensure there is no unregister/re-register activity on the client (for example, do not restart publishing/subscribing services, etc.).

- CSCth80893

  Symptoms: POE and Air Connect (AC) on a Cisco 892FW router do not work simultaneously. You cannot connect to the AC console when POE is powered on.

  Conditions: This symptom is observed on a Cisco 892FW router that has both POE and Air Connect with POE powered on.

  Workaround: There is no workaround.

- CSCth82293

  Symptoms: ISR-G2 router crashes due to bus error at PC 0x0 with spurious errors and the following message:

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

  Conditions: The symptom is observed with wrong usage of CNS initial and partial configurations mixed with **cns config retrieve** execution.

  Workaround: Avoid wrong CNS usage. Consult Cisco for correct CNS usage.

  Further Problem Description: Although the issue is seen with a Cisco 2911, it is not specific to the 2900 series alone. It can occur with any router platform.

- CSCth83508

  Symptoms: When performing an SRE install over WSMA, the router crashes and reboots.

  Conditions: The problem is seen when using WSMA to run the **session install** command.

  Workaround: Perform the install manually from a VTY session.

- CSCth84995

  Symptoms: Router may reload when performing an ISSU upgrade or downgrade.

  Conditions: This symptom occurs when performing an ISSU upgrade or downgrade.

  Workaround: There is no workaround.

- CSCth85829

  Symptoms: On an async tunnel, enabling “ip cef” can introduce latency/packet drop. You will see the following:

  - Packet loss is observed for CEF-switched traffic.
  - Very high latency is seen for successful packets.

  Conditions: The symptom is observed when:

  - “ip cef” is enabled.
  - Service-policy is attached to either dialer or async interface.

  Workarounds:

  1. Disable “ip cef”.
  2. Remove service policy from async interface.
  3. Use record option for ping from LAN host.
  4. Use a mainline code, for example: Cisco IOS Release 12.4(25).

- CSCth86402

  Symptoms: When flapping a WAN interface, the PIM tunnel disappears.

  Conditions: This happens when flapping a WAN interface after a few hours of working.

Workaround: Disable multicast routing, then enable it again.

- CSCth87587

  Symptoms: Spurious memory access or a crash is seen upon entering or modifying a prefix-list.

  Conditions: The primary way to see this issue is to have “neighbor <neighbor address> prefix-list out” configured under “address-family nsap” under “router bgp” when configuring/modifying a prefix-list.

  Workaround: There is no workaround.

  Further Problem Description: The issue is only specific to certain scenarios when prefix-lists are used in conjunction with “nsap address-family”.

- CSCth87638

  Symptoms: WIC-based platforms that have a MAC address with a leading 1 does not allow traffic to flow through the card successfully.

  Conditions: The symptom is observed on WIC-based platforms. It was seen originally on 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.

- CSCth89241

  Symptoms: Router crash with memory corruption pointing to the DNS resolution for IM servers.

  Conditions: The symptom is seen with a firewall policy configured with IM inspection and the IM filter was configured with domain names for address resolution.

  Workaround: Remove the protocol-info parameter-map attached to the IM match filter.

- CSCth90593

  Symptoms: A Cisco Router may crash from a corrupted program counter: “%ALIGN-1-FATAL: Corrupted program counter” from an IPIP call.

  Conditions: This symptom is observed only when the router is acting as a voice gateway.

  Workaround: There is no workaround.

- CSCth91093

  Symptoms: Exact symptom due to memory corruption is unknown at this time.

  Conditions: This symptom is observed after an L2TP HA switchover when L2TP retransmission takes a long time.

  Workaround: There is no workaround.

- CSCth91984

  Symptoms: Standby resets continuously.

  Conditions: This symptom is observed when 32 extended communities are configured with the **set extcommunity** command on the active RP.

  Workaround: Unconfigure the **set extcommunity** command.

- CSCth94827

  Symptoms: IDBINDEX_SYNC-STDBY tracebacks are seen when unconfiguring ima- group on a SONET-ACR controller.

Conditions: This symptom is observed on a standby supervisor when unconfiguring and configuring ima-group on a SONET-ACR controller.

Workaround: There is no workaround.

- CSCth99237

  Symptoms: LNS does not respond to an LCP echo reply when waiting for a response from the AAA server. As a result, the peer may close the session.

  Conditions: The symptom is observed under the following conditions:

  1. If the client starts to send LCP echo requests during the PPP Authentication phase.
  2. If the primary AAA server is unreachable and/or the authentication response is otherwise delayed.

  Workaround: There is no workaround.

- CSCti01692

  Symptoms: A Cisco ASR1000 crashes upon show run.

  Conditions: This symptom is observed with parser config cache interface enabled.

  Workaround: Disable the parser config cache interface.

- CSCti01971

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

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

  Workaround: There is no workaround.

- CSCti04670

  Symptoms: A crash may occur while the system is in flux with iEdge sessions going up and down while at the same time the **show ssm** command is issued on the console.

  Conditions: This symptom is seen when issuing the **show ssm** command.

  Workaround: Issue the **show ssm** command and then show logging to see the results.

- CSCti04754

  Symptoms: PPPoE sessions are stuck at attempting state forever.

  Conditions: This symptom is seen when sessions are triggered during SSO time, which get stuck at attempting state.

  Workaround: Clear attempting state sessions by the **clear** command from box.

- CSCti05663

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

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

  Workaround: There is no workaround.

- CSCti06686

  Symptoms: On a Cisco 2900, the async interface drops all outbound packets.

  Conditions: This symptom is observed with data packets that are exiting the async interface through the CEF path.

  Workaround: Disable hardware framing under the async interface using the following hidden command:

no ppp microcode

- CSCti07805

  Symptoms: Router reloads @sipSPIUpdSrtpSession.

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

  Workaround: There is no workaround.

- CSCti08115

  Symptoms: The removal of a port-channel interface associated with **mpls ldp advertise-labels interface Port-channelN** can cause a “config sync” error upon an SSO.

  Conditions: The symptom is observed after doing an SSO following the removal of the port-channel interface.

  Workaround: Before the SSO, remove the offending advertise-labels command when removing the port-channel command with:

  no interface Port-channelN no mpls ldp advertise-labels interface Port-channelN

- CSCti08336

  Symptoms: PfR moves traffic-class back and forth between primary and fallback links the when PfR Link group feature is used.

  Conditions: The symptoms are most likely to occur when there is one exit in the primary link-group and utilization is one of the criteria. The issue can also occur when there are two links in the primary. A traffic-class is moved from the primary link to the fallback link when the primary link is OOP. After the move, the primary link and the fallback link are “IN” policy. At that time, PfR moves the traffic-class back to primary causing the primary link to go “Out” of policy.

  Workaround: There is no workaround.

- CSCti08811

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

  Conditions: This symptom is observed only with EEM policies.

  Workaround: There is no workaround.

- 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.

- 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 following command: “switchport trunk allowed vlans except <mcast vlan#>”; or
2. Upgrade to Cisco IOS Release 15.1(2)T1.

- CSCti10518

  Symptoms: Under very rare circumstances, EIGRP could exhibit a memory leak of NDB structures in the RIB.

  Conditions: If redistribution is occurring into EIGRP and the route ownership is changing in the middle of the redistribution process, EIGRP may leak the NDB in process.

  Workaround: There is no workaround.

- CSCti10726

  Symptoms: A Cisco router reloads when it is configured for IPSec tunnel and the **show ip nbar protocol-d top-n** command is entered.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(2.9)T and configured for IPSec tunnel.

  Workaround: There is no workaround.

- CSCti10828

  Symptoms: In Cisco IOS Release 12.4T, there is no response to SNMP queries of:

  ```
  1.3.6.1.4.1.9.9.276.1.1.2.1.11 cieIfSpeedReceive 1.3.6.1.4.1.9.9.276.1.1.2.1.12
  cieIfHighSpeedReceive
  ```

  within the CISCO-IF-EXTENSION-MIB although supported at the CLI:

  ```
  interface GigabitEthernet0/3 bandwidth receive 100 <<<<<
  ==> BW 100000 Kbit/sec, RxBW 100 Kbit/sec
  ```

  Conditions: This symptom is observed under normal conditions.

  Workaround: There is no workaround.

- CSCti13286

  Symptoms: Putting this configuration on a router:

  ```
  router rip version 2 no validate-update-source network 10.0.0.0 no auto-summary !
  address-family ipv4 vrf test no validate-update-source network 172.16.0.0 no
  auto-summary version 2 exit-address-family
  ```

  and doing a reload causes the “no validate-update-source” statement to disappear from the VRF configuration (the one under the global RIP configuration remains). This affects functionality, preventing the RIP updates in VRF from being accepted.

  Conditions: The symptom has been observed using Cisco IOS Release 15.0(1)M3 and Release 15.1(2)T.

  Workaround: There is no workaround.

- 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.

- CSCti17190

  Symptoms: A router crashes when trying to do sre install.

Conditions: This symptom occurs when the TCL file has some missing attributes. The sre install fails and crashes the router.

Workaround: There is no workaround.

- CSCti18510

  Symptoms: Skinny phone registration fails when it is connected to a NAT router.

  Conditions: The symptom is observed with skinny (SCCP) phone traffic passing through a NAT router (where PAT is configured).

  Workaround: There is no workaround.

- CSCti18745

  Symptoms: If user has configured http port 80 or default http port, then reboots the router, it will produce invalid connection url with port 0. Later the connection from ACS to CPE might fail.

  Conditions: This symptom occurs if user has default http port 80 configured and then reboots the router.

  Workaround: Once router is up and running, again configure some port other than 80, and then reconfigure port 80.

  ```
  Router(config)#ip http port 8000
  Rotuer(config)#no ip http port or ip http port 80
  ```

- CSCti19627

  Symptoms: Extension assigner (EA) application erroneously exits after the first digit of the password is entered.

  Conditions: The symptom is observed when “call-park system application” is configured under telephony-service.

  Workaround: Remove “call-park system application”.

- CSCti22091

  Symptoms: Traceback will occur after a period of use and when the **show oer master** command is used a few times. The traceback is always followed by the message “learning writing data”. The traceback causes the OER system to disable. Manually reenabling PfR will not work. A reboot is required.

  Conditions: The symptom is observed when PfR is configured with the following conditions:

  1. list > application > filter > prefix-list
  2. Learn > traffic-class: keys
  3. Learn > traffic-class: filter > ACL

  Workaround: There is no workaround.

- CSCti22190

  Symptoms: The EIGRP autonomous system command does not NVGEN.

  Conditions:

  ```
  interface Tunnel2 ip vrf forwarding vpn2 no ip next-hop-self eigrp 10
  ```

  Now configure the address-family ipv4 command under legacy mode. For example:

  ```
  router eigrp 10 no auto-summary address-family ipv4 vrf vpn2 no auto-summary
  ```

  Now show the running configuration; the autonomous system command is not NVGENed.

  Workaround: Use the “address-family ipv4 vrf vpn2 autonomous 10" command.

- CSCti24577

  Symptoms: System crashes on active or hangs on standby.

  Conditions: The symptom is observed when a banner command is in the configuration.

  Workaround: Remove all banner commands.

- CSCti25063

  Symptoms: Call drops after codec change through midcall INVITE.

  Conditions: This issue occurs when both the codec and direction are changed compared to previous negotiated SDP. This is seen when using Cisco Unified Border Element (CUBE) with Cisco IOS Release 15.1(2)T. See the following topology:

  ```
  SIP(1) -- CUBE -- SIP(2)
  ```

  Codec G711 is negotiated. Next on SIP(2) midcall INVITE is received with updated SDP. CUBE detects updated SDP but when sending out INVITE on SIP(1), the SDP still has previous codec G711.

  Workaround: There is no workaround.

- CSCti25280

  Symptoms: An outgoing ISDN call with the module HWIC-2CE1T1-PRI might fail with this error message:

  ```
  **ERROR**: call_setup_ack_proceeding: NO HDLC available b channel 30 call id 0x8007
  ```

  Conditions: The symptom is observed when there is also a VWIC installed in the chassis (example: VWIC2-2MFT-T1/E1). This issue only happens on an ISR G2 router (Cisco 1900/2900/3900 series routers).

  Workaround: Remove the VWIC.

- CSCti25780

  Symptoms: One of the case values in the EIGRP registry is corrupted. This is seen right after bootup.

  Conditions: This symptom is observed when some of the files are compiled with optimization.

  Workaround: The corruption is not seen if the files are compiled with optimization disabled.

- CSCti26202

  Symptoms: With a Cisco 3900 series router, Modular Exponent (ModExp) is currently done using software and this leads to bad scalability.

  Conditions: The symptom is observed on a Cisco 3900 series router.

  Workaround: There is no workaround.

- CSCti26852

  Symptoms: Router crashes at ppp_sip_sw_session_cleanup.

  Conditions: The symptom is observed with multilink PPP scaled configurations and with a Cisco 7600 series platform. The crash may be seen following a SPA OIR. The crash decode is:

  ```
  sw_mgr_sm_valid_seg_class (seg_class=0x30343408) at
  ../xconnect/seg_sw_mgr_util.c:443 #1 0x120ab814 in sw_mgr_get_segtype
  (seg_class=0x30343408) at ../xconnect/seg_sw_mgr_util.c:478 #2 0x1435cd2c in
  ssf_dp_drop_remove_L2_context (seg1_class=0x30343408) at
  ../machine/../sss/ssf_switching_registry.regh:173 #3 0x1435d48c in
  ssf_dp_remove_dp_only_L2_features (seg_class=0x30343408) at
  ../sss/ssf_switching_util.c:113 #4 0x11c850f8 in ppp_sip_sw_session_cleanup
  (session=0x3a1c54f0) at ../VIEW_ROOT/cisco.comp/ppp/core/src/ppp_sip_switching.c:537
  ```

  Workaround: There is no workaround.

- CSCti27128

  Symptoms: A Cisco 2911 router crashes repeatedly when trying to boot up.

  Conditions: This symptom occurs when an IPVS module is installed in the NME slot with an SM-NM adaptor in a Cisco 2911 router. The Cisco 2921 is not affected.

  Workaround: There is no workaround if the IPVS module is required. Otherwise, the IPVS module can be removed from the Cisco 2911.

- CSCti31984

  Symptoms: A Cisco router crashes.

  Conditions: This symptom is observed when "Show stats" is used to show an auto ethernet monitor operation.

  Workaround: There is no workaround.

- CSCti33461

  Symptoms: The shared-line free call queue size is not able to reduce and eventually reaches the maximum limit.

  Conditions: The symptom is observed when only one active phone for a shared- line is up or when shared-line is configured for a single SIP phone.

  Workaround: Remove shared-line configuration and reconfigure to reset the queue size to 0.

- CSCti34627

  Symptoms: This bug is caused by a problem with the fix for CSCth18982. When a neighbor in multiple topologies is enabled, the open sent for the base topology clears the nonbase topology session for the same neighbor.

  Conditions: A GR-enabled neighbor exists in different topologies, one of them being the base topology.

  Workaround: Disable GR.

- CSCti34795

  Symptoms: In RA mode, SCEP enrolment requests stay in pending status. They will not time out automatically and cannot be cancelled with the **no crypto pki enroll** <*tp*>.

  Conditions: The symptom is observed when “enrollment mode ra” is configured under the Trust-Point.

  Workaround: Do not use RA mode, although in certain environments it is not scalable.

- 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

- CSCti41615

  Symptoms: Cisco 1941, 2901, 2911, or 2921 platforms disable ECC detection when a DIMM1 is installed. Any DRAM bit errors will not be detected/corrected.

Conditions: The symptom is observed on a Cisco 1941, 2901, 2911, or 2921.

Workaround: There is no workaround.

- CSCti45042

  Symptoms: When the **reload warm file flash0:**<*image*> command is issued on a Cisco 3900e router, the router does not boot the specified image due to "System received a Bus Error exception."

  Conditions: This symptom is observed in a Cisco IOS Release 15.1(2.13)T image when the **reload warm file flash0:**<*image*> command is issued.

  Workaround: There is no workaround.

- 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

- CSCti47649

  Symptoms: A router may crash with the message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x43563D04
  ```

  Conditions: The symptom is observed when the IOS DHCP server is enabled and DDNS updates are configured on the DHCP server.

  Workaround: There is no workaround.

- CSCti48014

  Symptoms: A device reloads after executing the **show monitor event** <*comp*> ... **all detail** command (where <*comp*> is an option listed under **show monitor event**?).

  Conditions: This symptom is observed if the configurations are done in the order below,

  monitor event-trace <*comp*> **stacktrace** <*depth*> **monitor event-trace** <*comp*> **size** <*size value*>

  and any related event gets recorded in between the above two configurations.

  Workaround: To avoid the crash, change the order of the above configurations; that is, configure the **size** command first and then configure the **stacktrace** command.

- 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.

- CSCti50740

  Symptoms: RSVP to No-RSVP interworking is not functioning correctly.

  Conditions: The symptom is observed when a media high-density transcoder option is enabled but not required.

  Workaround: Disable “media high-density transcoder”.

- CSCti54173

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

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

  Workaround: There is no workaround.

- CSCti55261

  Symptoms: On a phone button that has an overlay with call waiting DNs configured while the first call is connected, there is no audio on the second call and the first call gets disconnected after few seconds. The issue occurs when the second call comes in.

  Conditions: The symptom is observed on a phone button that has an overlay with call waiting DNs and when one DN is at hold state and the other is at connected state. It is seen with a CME that is running Cisco IOS Release 15.1(2)T1.

  Workaround: There is no workaround.

- CSCti57902

  Symptoms: IO memory corruption is seen when the image size expands.

  Conditions: The symptom is observed when the image size expands.

  Workaround: Leave the IO memory to the default (smart init).

- CSCti58272

  Symptoms: A PKI server with the **grant auto trustpoint** command will crash on client re-enrolment if PKI-AAA is enabled on the trustpoint associated with the **grant auto** command.

  Conditions: If trustpoint “pki-trustpoint” contains an authorization list PKI- AAA option, and pki-trustpoint is used as the “grant auto trustpoint” option on the PKI server:

  ```
  ! crypto pki server ca-server ... grant auto trustpoint pki-trustpoint ... crypto pki trustpoint pki-trustpoint authorization list aaa !
  ```

  The device crashes whenever a re-enrolment attempt is made to the PKI server.

  Workaround: Remove authorization list from the trustpoint (and skip the PKI- AAA process).

- CSCti62226

  Symptoms: Voice port(s) that are created with PRI/ds0 configurations are active even after shutting down those ports. Because of this, unconfiguring PRI/ds0 configurations throws an error.

  Conditions: The symptoms are observed with Cisco IOS Release 15.0(1)M3 when shutting down the voice-port to unconfigure the controllers.

  Workaround: Do **no shut** first then **shut**.

Further Problem Description: If you are running a script for regression which cannot be changed there is no workaround. If it is a user interactive case, the above workaround may help.

- CSCti62267

  Symptoms: An IPv6 CEF output is not seen in SP.

  Conditions: This symptom is observed when IPv6 is configured on UUT. This symptom is not observed with Ping.

  Workaround: There is no workaround.

- CSCti62913

  Symptoms: IP SLA repeatedly sends traps.

  Conditions: This symptom is observed in Cisco IOS Release 15.1T when IP SLA probes start failing and the router is configured to send traps, as in the following sample configuration:

```
ip sla 1 icmp-echo 10.22.22.22 source-ip 10.11.11.11 threshold 2000 timeout 2000
frequency 3 ip sla schedule 1 life forever start-time now ip sla
reaction-configuration 1 react timeout threshold-type consecutive 3 action- type
trapOnly
```

  Workaround: There is no workaround.

  Further Problem Description: When reaction condition is reached, a flag should be set and only one probe should be sent. No additional traps should be sent until the flag is set.

- CSCti67447

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

  Conditions: The symptom is observed under the following conditions:

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

  Workaround: There is no workaround.

- CSCti68721

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

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

  Workaround: If the symptom occurs, repeat the command.

- CSCti69008

  Symptoms: When dampening is configured for many VRFs, doing full vpnv4 radix tree walk and the proposed fix improves convergence by doing subtree walk based on VRF/RD.

  Conditions: Dampening configuration changes for VRFs.

  Workaround: There is no workaround.

- CSCti72836

  Symptoms: The router crashes when removing an ACL.

  Conditions: The symptom is observed when the ACL has some IP addresses that index to 127 in the hashtable.

  Workaround: There is no workaround.

- CSCti80904

  Symptoms: A router reloads at sec_send_command while booting up.

  Conditions: The symptom is observed on a Cisco 887 and a Cisco 888 router.

  Workaround: There is no workaround.

- CSCti86169

  Symptoms: A device that is acting as a DHCP relay or server crashes.

  Conditions: This symptom is observed when the “no service dhcp” command is configured.

  Workaround: There is no workaround.

- 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.

- CSCti92798

  Symptoms: A Cisco router crashes while configuring http commands with atm.

  Conditions: This symptom is observed on a Cisco7200 router running Cisco IOS Release 15.1(2)T.

  Workaround: There is no workaround.

- CSCti93398

  Symptoms: A Cisco 1861 router reloads.

  Conditions: The reload occurs upon booting.

  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.

- CSCtj06390

  Symptom: Ping fails after configuring crypto.

  Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(2.18)T.

  Workaround: There is no workaround.

- CSCtj07125

  Symptoms: Cisco IOS WAAS Express uses the burned-in MAC address of the first Ethernet interface as its own local device ID. This device ID is sent as a router identifier to the WAAS Central Manager (WCM) and is communicated to other WAAS peers during autodiscovery.

  On Cisco 1941W platforms, the burned-in MAC address of the first Ethernet interface is 0000.0000.0007, which happens to be the same for all Cisco 1941W routers.

  This will cause the WCM to have two routers that are registered with the same client ID. It might also affect IOS-WAAS operation.

  Conditions: This symptom is observed while registering WAAS on Cisco 1941W platforms with the WCM and enabling WAAS on these platforms.

  Workaround: There is no workaround.

- CSCtj20106

  Symptoms: Router crashes upon removing “ip flow monitor” from an interface.

  Conditions: The symptom occurs on a Cisco 7200 series router that is running Cisco IOS interim Release 15.1(2.19)T.

  Workaround: Enable “protocol-discovery” on the interface and then configure “flow monitor”.

- 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 that receives the keepalive segment is getting dropped by the ZBF.

  Conditions: The symptom is observed when you have TCP connections using keepalive going over a ZBF implementation.

  Workaround: Shorten the keepalive timeout on the other endpoint.

- CSCtj22125

  Symptoms: NBAR is not disabled and does not free resources.

  Conditions: The symptom is observed when “protocol-discover” is configured and unconfigured.

  Workaround: There is no workaround.

- CSCtj25649

  Symptoms: Inline power to ip phone fails on NM-16-ESW and NMD-36-ESW

  Conditions: This symptom is seen on NM-16-ESW and NMD-36-ESW that is using a Cisco IOS Release 15.1(2)T1.1 image.

  Workaround: There is no workaround.

- CSCtj31743

  Symptoms: Memory leaks@slaAddSeqNum are seen.

  Conditions: This symptom is observed when "pfs border" is configured.

  Workaround: There is no workaround.

- CSCtj32574

  Symptoms: Deleting the **redistribute** command into EIGRP does not get synchronized to the standby. For example:

  ```
  router eigrp 1 redistribute connected no redistribute connected
  ```

The **no redistribute connected** command is not being backed up to the standby.

Conditions: The symptom is observed with any redistribute-related commands.

Workaround: There is no workaround.

- CSCtj38327

  Symptoms: Router crashes due to NBAR configuration.

  Conditions: The symptom is observed when **ip nbar protocol- discovery** is applied to the tunnel interface.

  Workaround: There is no workaround.

- CSCtj38346

  Symptoms: Router crash is seen when configuring the **default transmit- interface** command.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.1(2.19)T.

  Workaround: There is no workaround.

- CSCtj39664

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

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

  Workaround: There is no workaround.

- CSCtj53363

  Symptoms: A Cisco router hangs indefinitely and the console does not respond.

  Conditions: The symptom is observed with the following conditions:

  - AIM-VPN in ISR + ZBFW; or
  - A Cisco 2811/2821 Onboard VPN + ZBFW

  Once traffic starts, the router hangs within minutes.

  Workaround: If the device is a Cisco 2811/2821, use sw crypto + ZBFW.

  Alternate Workaround: If the device is a Cisco 2851 or higher ISR, use onboard crypto + VPN instead of AIM-VPN + ZBFW.

- CSCtj76297

  Symptoms: Router hangs with interoperability of VM and crypto configurations.

  Conditions: The symptoms are seen only during interoperability between video- monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

  Workaround: Disable AIM and use onboard CE.

- CSCtj94617

  Symptoms: A mem leak occurs when the **show runnning/ show ip access-list** command is entered.

  Conditions: This symptom is observed even without a named ACL configured on the device.

  Workaround: There is no workaround.

  Further Problem Description: The mem leak occurs in a dynamic list that is not destroyed properly.