Caveats for Cisco IOS Release 15.2(4)S

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 section consists of the following subsections:

Using the Bug Search Tool

The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested. In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

For more information about how to use the Cisco Bug Search Tool, including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. if you do not have one, you can register for an account.

To use the Cisco Bug Search Tool:

1. In your browser, navigate to the Cisco Bug Search Tool.
2. If you are redirected to a **Log In** page, enter your registered Cisco.com username and password and then, click **Log In**.
3. To search for a specific bug, enter the bug ID in the **Search For** field and press Enter.
4. To search for bugs related to a specific software release, do the following:
   a. In the **Product** field, choose **Series/Model** from the drop-down list and then enter the product name in the text field. If you begin to type the product name, the Cisco Bug Search Tool provides you with a drop-down list of the top ten matches. If you do not see this product listed, continue typing to narrow the search results.
   b. In the Releases field, enter the release for which you want to see bugs.

   The Cisco Bug Search Tool displays a preview of the results of your search below your search criteria. You can mouse over bugs to see more content about a specific bug.
5. To see more content about a specific bug, you can do the following:
   - Mouse over a bug in the preview to display a pop-up with more information about that bug.
   - Click on the hyperlinked bug headline to open a page with the detailed bug information.
6. To restrict the results of a search, choose from one or more of the following filters:

Filter	Description
Modified Date	A predefined date range, such as last week or last six months.
Status	A specific type of bug, such as open or fixed.
Severity	The bug severity level as defined by Cisco. For definitions of the bug severity levels, see Bug Search Tool Help & FAQ
Rating	The rating assigned to the bug by users of the Cisco Bug Search Tool.
Support Cases	Whether a support case has been opened or not.

Your search results update when you choose a filter.

All resolved bugs for this release are available in the Cisco Bug Search Tool through the fixed bug search.

This search uses the following search criteria and filters:

Field Name	Information
Product	Series/Model Cisco IOS and NX-OS Software => Cisco IOS
Release	15.4(2)S2

Field Name	Information
Status	Fixed
Severity	2 or higher

Resolved Caveats—Cisco IOS Release 15.2(4)S7

Table 1 Resolved Caveats—Cisco IOS Release 15.2(4)S7

Identifier	Description
CSCus48378	POODLE: CNS feature required to support TLS
CSCup34371	GETVPN GM stops decrypting traffic after TEK rekey
CSCul70788	Router crashes when calculating the best cost successor in EIGRP DUAL
CSCur13495	Service-data of a service change is not updated by SAF forwarder
CSCur43251	POODLE protocol-side fix: HTTPS Client
CSCuo84660	copy command yields DATACORRPUTION error
CSCuh07579	IPSec fails to delete/create SAs due to IPSec background process stuck
CSCuo95771	IPSec SA are deleted incorrectly by background process
CSCua01375	ldap VRF is not working with PKI
CSCus48386	POODLE related fix: LDAPv3 client REQUIRED to support TLS
CSCur23656	Cisco IOS and IOSd in IOS-XE: evaluation of SSLv3 POODLE vulnerability
CSCup32531	Both ESPs crash at AOM Parent when flapping 6K flexvpn sessions

Resolved Caveats—Cisco IOS Release 15.2(4)S6

- CSCtg57599

  Symptom: Lots of SNMP CPUHOG messages are seen and there is a crash due to a watchdog timeout:

  ```
  %SYS-3-CPUHOG: Task is running for (126004)msecs, more than (2000)msecs
  (252/37),process =SNMP ENGINE
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SNMP ENGINE
  ```

  Conditions: Device is configured with SNMP and is polled for Dot3Stats.

  Workaround 1: Use the following command: **no snmp-server sparse-tables**.

  Workaround 2: Block the objects in dot3 mib that contains this table from being polled:

  ```
  snmp-server view cutdown iso included
  snmp-server view cutdown 1.3.6.1.2.1.10.7 excluded
  ```

  Then to apply the view, use:

  ```
  no snmp-server community your_string_here RO
  no snmp-server community your_string_here RW
  ```

  and then put it back so it looks like:

  ```
  snmp-server community your_string_here view cutdown RO
  snmp-server community your_string_here view cutdown RW
  ```

Further Problem Description: Cisco IOS Software contains a vulnerability that could allow an authenticated, remote attacker to trigger a high CPU on the device via walking specific SNMP objects.

The vulnerability is due to an uninitialized variable in the code. An attacker could exploit this vulnerability by performing SNMP walks against objects on the affected device. An exploit could allow the attacker to cause high CPU on the affected devices.

This vulnerability is not consistently exploitable.

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-2012-5030 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

- CSCtq23960

  Symptoms: A Cisco ISRG2 3900 series platform using PPC architecture crashes and generates empty crashinfo files:

  ```
  show flash: all
  -#- --length-- -----date/time------ path <<snip>> 2 0 Mar 13 2011 09:40:36
  crashinfo_<date> 3 0 Mar 13 2011 12:35:56 crashinfo_<date> 4 0 Mar 17 2011 16:14:04
  crashinfo_<date> 5 0 Mar 21 2011 05:50:58 crashinfo_<date>
  ```

  Conditions: The symptom is observed with a Cisco ISRG2 3900 series platform using PPC architecture.

  Workaround: There is no workaround.

- CSCtu42387

  Symptoms: Gigabit and 10 Gigabit Fiber link reporting threshold violation alarm in Cisco ME3600, Cisco ME3800, and Cisco 7600 devices. The "%SFF8472-3-THRESHOLD_VIOLATION: Gi0/11: Rx power high alarm" error message is seen on ports.

  Conditions: This symptom is observed on Cisco ME3600, Cisco ME3800, and Cisco 7600 devices. The messages are seen with the interface shut or no shut.

  ```
  SFF8472-3-THRESHOLD_VIOLATION Gi5/1: Rx power low alarm; Operating value: -28.5 dBm,
  Threshold value: -24.0 dBm
  ```

  Workaround: Fixing the fiber signal issue or disconnecting the fiber from the transceiver has been known to stop the messages.

- CSCtv21900

  Symptoms: Intermittent one-way audio occurs from an MGCP gateway to a Cisco IP phone.

  Conditions: This symptom is observed under the following conditions:

  - Encrypted call with SRTP - MGCP Controlled Gateway
  - Cisco IOS Release 15.1(4)M or later releases

  Phone logs show the following message:

  ```
  6622: DBG 23:29:50.256330 DSP: RTP RX: srtp_unprotect() again 6623: DBG
  23:29:50.257139 DSP: RTP RX: srtp_unprotect() failed with error code 7 6624: DBG
  23:29:50.276390 DSP: RTP RX: srtp_unprotect() failed with auth func 3
  ```

The “Rcvr Lost Packet” counter on the Cisco IP phone begins to increment as soon as the call connects.

Workaround 1: Downgrade the software to Cisco IOS Release 15.1(3)T or earlier releases.

Workaround 2: Perform a hold/resume on the one-way audio call. This mitigates the problem.

- CSCty16106

  Symptom: IKE/GDOI bypass policy entries (four entries) are downloaded to PAL dataplane SADB as part of the initial policy download. But, as IKE/GDOI traffic is never routed to tunnel interfaces, the entries are not required for tunnel protection cases.

  Conditions: This symptom is observed with IKE/GDOI bypass policy entries.

  Workaround: There is no workaround.

- CSCtz97771

  Symptom: During regular operations, a Cisco router running Cisco IOS release 12.4(24)T and possibly other releases experiences a crash. The crash info will report the following:

  ```
  %SYS-2-FREEFREE: Attempted to free unassigned memory at 4A001C2C, alloc 4180794C,
  dealloc 417616B0,
  %SYS-6-BLKINFO: Attempt to free a block that is in use blk 4A001BFC, words 134, alloc
  4180794C, Free, dealloc 417616B0, rfcnt 0,
  ```

  Conditions: This symptom is not observed under any specific conditions.

  Workaround: There is no workaround.

- CSCuc60868

  Symptom: A router randomly crashes either due to memory corruption at bgp_timer_wheel or memory chunks near bgp_timer_wheel (For example, BFD event chunks if BFD is configured or AtoM Manager chunks if LDP is configured). A crash occurs right after an LDP neighbor is up in the L2VPN setup.

  Conditions: This symptom occurs when **vpls bgp signaling** is unconfigured and then reconfigured. Both L2VPN and BGP are unconfigured and reconfigured after all L2VPN and BGP data structures are fully deleted (about 3 minutes for 5 BGP VPLS prefixes). For the repro on file, OSPF (for IGP) is also unconfigured and reconfigured. Both LDP and BGP signaling are affected by this caveat.

  Workaround: Avoid unconfiguring and reconfiguring BGP L2VPN.

- CSCud25043

  Symptoms: A WebVPN-enabled gateway crashes on Cisco IOS Release 15.1(4)M5 due to SSLVPN_PROCESS.

  Conditions: This symptom is observed under the following conditions:

  - Cisco IOS Release 15.1(4)M5
  - SSL VPN (WebVPN enabled)

  Workaround: There is no workaround.

- CSCud55435

  Symptom: Optimization of AAA and RADIUS function calls.

  Conditions: This symptom occurs when AAA APIs are optimized based on X-ray reports.

  Workaround: There is no workaround.

- CSCud62864

  Symptom: When the Mid-call Re-INVITE consumption feature is active, CUBE consumes Re-INVITE which should change the media state from “sendonly” to “sendrcv”. This results in a one way or no way audio on the call.

  Conditions: This symptom occurs when the CUBE Mid-call Re-INVITE consumption feature is enabled.

  Workaround: There is no workaround.

- CSCud86991

  Symptom: On ASR1K, the IOSd process may crash with “crypto dynamic-map” configuration.

  Conditions: This symptom is observed When “crypto dynamic-map ...” configuration is entered from CLI.

  Workaround: There is no workaround.

- CSCue06450

  Symptom: If NTP is not configured on a Cisco ASR 1000 Series router, then PKI (Public Key Infrastructure) services such as auto enrollment and certificate rollover may not function correctly due to an invalid clock.

  Conditions: This symptom occurs if NTP is not configured, or if NTP is not synchronized to the NTP server.

  Workaround: Enable NTP on the router.

- CSCue23898

  Symptom: A Cisco router running Cisco IOS Release 15.3(1)T may crash with a bus error immediately after issuing the **write memory** command.

  ```
  Example: 14:44:33 CST Thu Feb 14 2013: TLB (load or instruction fetch) exception, CPU
  signal 10, PC = 0x228B2C70
  ```

  Conditions: This symptom occurs while updating the router’s running configuration with the **write memory** command.

  It is caused by this CLI command “ccm-manager redundant-host A.B.C.D A.B.C.D”. For example, “ccm-manager redundant-host 172.21.200.15 172.21.200.13”.

  Workaround: There is no workaround.

- CSCug37304

  Symptom: The problem was experienced the first time on a UC560 that was upgraded to Cisco IOS Release 15.1(4)M5.

  At the end of the investigation, it was determined that this is neither specific to the platform nor does it apply to Cisco IOS Release 15.1(4)M5.

  This problem is platform independent and all releases leading to the most current release on Cisco.com in Cisco IOS Release 15.1(4)M (most recent release on Cisco.com at the time writing this explanation is Cisco IOS Release 15.1(4)M7) are affected by this issue.

  Conditions: Crash is seen specifically when FXS ports are in STCAPP controlled mode.

  Workaround: Use the standalone FXS Port, rather than STCAPP controlled. Configure the FXS port as a standalone FXS port, if possible.

- CSCug47401

  Symptom: An RP crash is seen with 128K PWLAN sessions.

Conditions: This symptom is observed after trying to authenticate simple IP sessions with CoA

Workaround: There is no workaround.

- CSCuh05259

  Symptom: Prompt is provided for configure replace command when **file prompt quiet** is configured.

  Conditions: This symptom is observed when “file prompt quiet” has been configured.

  Workaround: Use “force” along with the **configure replace** command.

- CSCuh36124

  Symptom: Service Routing/SAF in Cisco IOS Release 15.2.X.X is experiencing HIGH CPU during a failover condition where the active SAF forwarder looses connection to the network causing the clients to switch to the secondary forwarder. This issue occurs if the forwarder, that becomes active, still has an active neighbor that it needs to send updated registration data to (so more than two forwarders are required to observe this defect). Due to the high CPU condition during this failover, clients can experience longer registration times increasing the outage window.

  Conditions: It has been validated in the lab, that the condition only occurs when more than two forwarders are involved and all the forwarders are peered to each other via direct configured peers or network based EIGRP peers. The HIGH CPU is caused directly by the connection that exists between SAF forwarders to exchange data across the network, and not due to the client towards SAF forwarder data exchange.

  Workaround: There is no workaround.

- CSCuh56385

  Symptom: Very slow propagation of data across a network of SAF forwarders after a fail over condition is observed. More than two SAF forwarders are required to observe this defect.

  Conditions: This symptom occurs when there are more than two SAF forwarders in the network. After a fail over condition and the clients initiate advertising patterns into the standby forwarder, the propagation of these advertisements via update messages to the SAF peers can experience a 5 second inter-service advertisement delay.

  Workaround: There is no workaround. Once the forwarder that suffered the fail over condition returns and establishes its neighbor relationships with its peers, the forwarders will update quickly.

- CSCuh68961

  Symptom: In a DO-DO scenario, the CUBE is not able to send re-invite on other leg if the CUBE receives re-invite immediately followed by ACK.

  Conditions: SIP (PSTN) -- CUBE -- SIP -- CUCM -- IP phone transfers to another IP phone Message Sequence in CUBE CUCM --> reINVITE --> CUBE --> reINVITE --> Provider <-- 200OK 200OK <-- ACK --> reINVITE --> --> ACK

  reINVITE from CUCM is not forwarded to the provider

  Workaround: There is no specific workaround. This issue is only seen from the Cisco IOS release 15.1(4)M and newer.

- CSCuh72000

  Symptom: The TOS of one kind of PIM signaling packet is set to 6. When the packet is encapsulated into MPLS, the TOS value is copied to the EXP value. The packet will then be encapsulated into GRE/IP again, but the EXP value is not copied. PI just leaves the TOS in the IP/GRE header 0.

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

- CSCuh87195

  Symptom: A crash is seen on a Cisco router.

  Conditions: The device crashes with gw-accounting and call-history configured. The exact conditions are still being investigated.

  Workaround: Perform the following workaround:

  1. Completely remove gw-accounting
  2. Disable call-history using the following commands:

```
gw-accounting file
no acct-template callhistory-detail
```

- CSCui04860

  Symptom: HA sync is not happening from active to standby.

  Conditions: This symptom is observed when HA Sync-up is not happening for PKI Server on Cisco IOS Release 15.3(2.25)M0.1.

  Workaround: There is no workaround.

- CSCui29745

  Symptom: Member links under MLPPP go down as the LCP negotiation of those PPP links fails.

  Conditions: This symptom occurs after the router reloads and the traffic is flowing through the multilink.

  Workaround: Reload SPA/LC on the other end of the link.

- CSCui51363

  Symptom: The multilink does not pass traffic even though it is in an up/up state.

  Conditions: This symptom occurs when the auto DNR status is set and the sip400 ucode crashes.

  Workaround: Perform a shut/no shut in the multilink.

- CSCui54359

  Symptom: Switchover to T.38 fax-relay does not occur when configured for SG3 fax calls. Calls switchover to fax passthrough.

  Conditions: This is observed when fax machines support the SuperG3 standard on both end and the voice gateways are configured to use H323 and T38 v3 fax relay.

```
example: dial-peer voice 1 voip
destination-pattern <did>
session target ipv4:<ip_address>
fax protocol t38 version 3
or
voice service voip
fax protocol t38 version 3
```

  Workaround: Use SIP as the VoIP protocol.

  Add “session protocol sipv2” to the voip dial-peer.

  If CUCM is involved, configure a SIP trunk for call handling from/to the voice gateway.

- CSCui59004

  Symptom: IOSd crashes while removing NTP server from the configuration.

  Conditions: This may occur rarely, when removing “ntp server <hosname>” from configuration. ntp servers configured with ip addresses will not cause the same.

Workaround: Timing the “no ntp” configuration such that it does not overlap with the 60 second DNS resolution timer.

- CSCui59927

  Symptom: A memory leak is observed on a Cisco device due to IPSec which causes free memory to deplete to an extent where the device becomes unreachable.

  Conditions: This symptom occurs when IPSec scaling is high.

  Workaround: Reduce scaling of IPSec sessions.

- CSCui64807

  Symptom: An active RP crashes during FIB sync because of memory overrun when the standby sup becomes unavailable.

  Conditions: This symptom occurs when redundant RPs are configured in SSO mode and the standby RP becomes unavailable (for instance because of crash or physical removal). The issue occurs only on Cisco 7600 RSP 720, Cisco 7600 Series Supervisor Engine 720, and Cisco 7600 platforms where the tableid “ISSU FOF LC” support is enabled. As of 03/17/2014, the tableid “ISSI FOF LC” feature is only supported on SY releases. This issue does not impact Cisco ASR 1000 Series platforms.

  Workaround: There is no workaround.

- CSCui85371

  Symptom: Ikev2 session is NOT coming UP.

  Conditions: This defect can be seen on an IKEv2 initiator only. The IKEv2 authentication mechanism is certificate based and a certificate map is configured under IKEv2 profile.

  Workaround: There is no workaround.

- CSCuj14595

  Symptom: A Cisco 3945 voice gateway running Cisco IOS Release 15.2(4)M3 or Cisco IOS Release 15.2(4)M4 may have a processor pool memory leak in the CCSIP_TCP_SOCKET process.

  Conditions: This symptom is seen on slow TCP connections, where the response is slow and frequent transmission errors are observed.

  Workaround: There is no workaround.

- CSCuj17818

  Symptom: PPPoE is configured on radio interfaces. When a shut and no shut are issued on remote interface Router2, nine packets get stuck in the Router1 input queue.

  Conditions: This problem is seen in Router1 when shut is issued on the Router2 interface to disconnect the PPPoE session between Router1 and Router2. In this case the Radio Emulator sends the PADQ packets to Router1 which gets stuck in input queue.

  Workaround: Reloading the box to clear the input queue.

- CSCuj19201

  Symptom: Re-registration time is recalculated on GM nodes upon receiving a TBAR rekey, based on the remaining TEK lifetime at the time of the TBAR rekey.

  This effectively causes a much-shorter re-registration window compared to the one obtained at the GM registration, even if the original TEK lifetime was configured with a long value.

  Conditions: This symptom is observed when TBAR is configured and long TEK lifetime used (more than 7200 seconds).

  Workaround: There is no workaround.

- CSCuj30572

  Symptom: With EIGRP and PFR configured, a Cisco router crashes after giving following EIGRP messages:

  ```
  000111: Sep 17 09:08:33.331: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.50.2.1
  (Tunnel502) is down: Peer Termination received 000112: Sep 17 09:08:33.347:
  %DUAL-3-INTERNAL: EIGRP-IPv4 1: Internal Error -Traceback= 319D4CB4z 319EC5E4z
  319EC7C8z 319E4950z 319EA760z 31A25008z 32C23084z 32C23068z
  ```

  Conditions: This symptom occurs when PFR, OER, and EIGRP are configured.

  Say RouterUnderTest has two EIGRP Peers HUB1 and HUB2. (Given metrics are only for illustration)

  When EIGRP has a Prefix with 3 different Paths installed in following order

  ```
  DRDB1 NH - HUB1, Metric 36571392 / 0 (Installed by PFR)
  DRDB2 NH - HUB2, Metric 58322432 / 409600 ( x Hops away learnt from RouterX)
  DRDB3 NH - HUB1, Metric 538004992/500409600 (y Hops away learnt from Router Y)
  ```

  With these initial conditions, if Neighbor ship with Router Y goes down, Both PFR and EIGRP try to delete DRDB3 Which results in inconsistent data structures with Memory corruption. Any further access to Memory will result in Crash.

  Workaround: No possible work arounds seen. Using other Load sharing methods instead of PFR looks only possible work around.

  More Info: Usually, the crash is seen during execution of EIGRP Route lookup function similar to below.

  ```
  0x33841E10:eigrp_pfr_get_drdb(0x33841ddc)+0x34
  0x33842014:eigrp_pfr_route_lookup(0x33841e88)+0x18c
  ```

- CSCuj62593

  Symptom: Gateway crashes with MALLOCFAIL during ASR/TTS load.

  Conditions: During longevity load for five days, crash is seen almost 61 hours into the load with Cisco IOS Release 15.3(3)M1 and almost 12 hours into load with Cisco IOS Release 15.2(4)M5, due to the non-optimal usage of memory.

  Workaround: There is no workaround.

- CSCuj72215

  Symptom:

  A vulnerability in handling of RTCP traffic of Cisco CUBE could allow an unauthenticated, remote attacker to cause traffic destined to an affected device as well as traffic that needs to be processed-switched to fail.

  The vulnerability is due to exhaustion of interface input queue by the RTCP traffic. An attacker could exploit this vulnerability by sending RTCP packet in a specific sequence. An exploit could allow the attacker to cause traffic destined to an affected device as well as traffic that needs to be processed- switched to fail.

  Conditions:

  RTCP packets have been found to be associated with SIP but any voice protocol may be involved.

  The default input queue size is 75 on ISR routers. When the input queue fills up, the size (76) will exceed the max. This may look like an input queue wedge on the surface but for this bug, the packets should be drained once the call is torn down and the socket is removed. The RTCP packets should

only be punted to the CPU for processing (and thus hit the input queue) when the RTP session isn't yet established and we don't have a socket. Once this establishment is done, RTCP traffic should be processed in the fast-path.

Workaround: To alleviate the problems caused by filling up the input queue, the size can be increased with the following command at the interface level, **hold-queue <size> in**.

To stop the issue altogether, RTCP would be need to be disabled by the voice endpoints.

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 5/4.1:
https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CVE ID CVE-2014-3268 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at:
http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-3268

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

- CSCuj82897

  Symptom: The "control-word" length is not set properly for small HDLC packets running over HDLC AToM VC with SIP-200. For example: SPA-8XCHT1/E1.

  Conditions: This symptom occurs when HDLC AToM VC with SIP-200 is deployed, for example, SPA-8XCHT1/E1, will result in a packet length mismatch issue or dropping by the remote PE router when HDLCoverMPLS runs over the Ethernet link adding an additional padding which cannot be classified at all.

  Workaround: Use SIP-400.

- CSCuj85382

  Symptom: ME3400 reload.

  Conditions: This symptom is observed under the following conditions:

  1. "ethernet cfm traceroute cache" configured.
  2. A Local only ethernet traceroute performed.

  Workaround: Disable CFM traceroute cache by removing "ethernet cfm traceroute cache" configuration.

- CSCuj87667

  Symptom: When value "xxx" of MPLS exp bits was copied to outer IP/GRE header TOS, the new TOS value should be "xxx00000" but now it is "00000xxx", so that the QoS information was broken.

  Conditions: This symptom is observed in MPLS over GRE case.

  Workaround: There is no workaround.

- CSCuj94571

  Symptom: To run the BERT test, remove "keepalive" from the interface. After completing the BERT test, adding "keepalive" causes the standby RSP to reset.

  Conditions: This symptom is consistent and affects Cisco IOS Release 15.1(3)S1.

  Workaround: After the completion of the BERT test, remove the BERT test with "no bert pattern qrss interval <interval>" and then add "keepalive". This will avoid standby RSP reset.

- CSCul27924

  Symptom: Customer experienced crash on ASR-1001 during normal operation.

  Conditions: This symptom is not observed under any specific condition.

  Workaround: There is no workaround.

- CSCul49375

  ```
  Symptom: The Cisco ASR 1000 router displays the following messages in the logs:
  %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0) -Traceback=
  1#cb40dca901558e45a65b881a8695af4f :400000+8653B3 :400000+893696 :400000+DF330C
  :400000+DED89B :400000+DF8643 :400000+1F57F36 :400000+1F4BBFB :400000+1F33BA7
  :400000+1F336C1 :400000+1F34FF9 :400000+1F27763 :400000+1F29B16 :400000+2546FF3
  :400000+2546EDD :400000+1F2930B
  ```

  No new PPPoE sessions can be established anymore.

  Conditions: The conditions to this symptom are unknown.

  Workaround: Reload the device.

- CSCul54254

  Symptom: Invalid LSAs are not flushed by the router which has their Advertising Router ID. Specifically, Router LSAs which do not have LSID of 0 will not be flushed if the router does not re-originate them, and any LSA with a type that the router does not recognize.

  Lingering LSAs could lead to incorrect routing in some very obscure instances. For example, stale Router LSA fragments from two neighboring routers would need to remain in the network. There would not be a routing problem if only one router's stale Router LSA fragment was allowed to linger.

  Conditions: There are several possible scenarios that could lead to this symptom. One example is that a router is configured with many interfaces attached to an OSPFv3 instance such that it originates more than one Router LSA fragment. Then the router is reloaded before the configuration is saved, and after the reload it does not reoriginate some of the Router LSA fragments.

  Workaround: There is no workaround.

- CSCul75876

  Symptom: A router may crash in an OSPF process during reconfiguration.

  Conditions: This symptom occurs under the following conditions:

  1. Configure the router with "ipfrr" in area 0.
  2. Connect router to area 0 through two links. For some route one interface is the primary path, and the second is the repair path.
  3. Configure router as ABR, that is, have a non-zero area with a neighbor. Do not configure "ipfrr" in the non-zero area. Quickly remove the IP address from both the interfaces in area 0 and router the may crash.

  Workaround: Changes to the reconfiguration procedure will avoid the crash.

  - Shutdown the interface before removing the IP
  - Remove the IP from one interface in area 0, wait for a few seconds and remove the IP address from the second interface in area 0.

- CSCul94087

  Symptom: Output Packet drops is observed on the ATM IMA interface even when there is no live traffic and only signaling exchange between non-Cisco devices. Although output drops in most cases means low bandwidth issues but in this case, an entire site was down due to these drops.

Conditions: This symptom occurs under the following conditions:

1. Layer 2 cross connect is configured on Cisco device and Non-Cisco device at other end.
2. Only signalling traffic flows through the devices.
3. IMA group is created for the ATM connectivity.
4. SPA-24CHT1-CE-ATM card is to be used for the ATM connection.

Workaround: Reload the SPA.

- CSCul96778

  Symptom: A router may crash and reload with BGP related traceback in an extremely rare timing condition while running “show ip bgp vpnv4 vrf XXXX nei A.A.A.A”.

  Conditions: While making BGP related changes such as moving the same neighbor with quick operation of “no neighbor x.x.x.x “ and then “neighbor x.x.x.x” across VRFs. Immediately after this if we type a “show ip bgp vpnv4 vrf XXXX nei A.A.A.A” on a Cisco router running IOS and BGP, then in extremely rare timing condition the router may crash. The possibility of this to happen increases if their configuration and unconfiguration is done from one console and the show operation done from other console.

  Workaround: When doing configuration and un-configuration and then show, its better to serialize the operation rather than aggressively use multiple consoles to do all actions at the same time.

- CSCum00056

  Symptom: ASR IOSd crash occurs with the following error:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = ISG CMD HANDLER
  ```

  Conditions: This symptom occurs when changes are made through RADIUS.

  Workaround: There is no workaround.

- CSCum02221

  Symptom: A vulnerability in BGP processing code of Cisco IOS could allow an unauthenticated, remote attacker to cause a reload of the affected device..

  The vulnerability is due to improper parsing of malformed BGP packets. An attacker could exploit this vulnerability by sending malformed BGP packets to an affected device. An exploit could allow the attacker to cause a reload of the affected device.

  Conditions: This symptom occurs when the device configured for BGP.

  Workaround: There is no workaround.

- CSCum14830

  Symptom: Leaking IPv6 routes is observed from a VRF table into the global table using BGP. These routes consist of the following: 1. BGP routes learned from the VRF IPv6 BGP peer. 2. Redistributed static and connected routes.

  The BGP routes leak fine, but the redistributed static and connected routes have an issue. After the redistributed routes leak, the exit interface shows “null0”. Sometimes instead of showing the exit interface as “null0”, it shows a random interface which is a part of VRF and has IPv6 enabled on it.

  Conditions: This symptom occurs with IPv6 redistributed connected and static routes into BGP VRF (could also be redistributed from other protocols as well but have not been tested).

  Workaround: There is no workaround.

- CSCum16315

  Symptom: Upon reload of a Cisco 7600 router configured with a CoPP policy containing IPv6 ACLs and DSCP matching, the CoPP is only applied to the active RSP as shown below.

  After reload:

```
lab-7609-rsp-02#sh mod power Mod Card Type Admin Status Oper Status ---
------------------------------------ ------------ ------------ 1 CEF720 48 port
10/100/1000mb Ethernet on on 5 Route Switch Processor 720 (Active) on on 6 Route
Switch Processor 720 (Hot) on on 7 CEF720 8 port 10GE with DFC on on 8 CEF720 8 port
10GE with DFC on on
```

  CoPP is applied to only the active RSP/SUP after reload:

```
lab-7609-rsp-02#sh mod power
Mod Card Type Admin Status Oper Status --- ------------------------------------
------------ ------------ 1 CEF720 48 port 10/100/1000mb Ethernet on on
5 Route Switch Processor 720 (Active) on on
6 Route Switch Processor 720 (Hot) on on
7 CEF720 8 port 10GE with DFC on on
8 CEF720 8 port 10GE with DFC on on
CoPP is applied to only the active RSP/SUP after reload:
lab-7609-rsp-02#sh policy-map control-plane in | inc class|Earl
class-map: COPPCLASS_MCAST (match-any)
Earl in slot 5 :
class-map: COPPCLASS_MGMT (match-any)
Earl in slot 5 :
class-map: COPPCLASS_ALLOW_ICMP (match-any)
Earl in slot 5 :
class-map: COPPCLASS_MONITORING (match-any)
Earl in slot 5 :
class-map: COPPCLASS_FILEXFER (match-any)
Earl in slot 5 :
class-map: COPPCLASS_REMOTEACCESS (match-any)
Earl in slot 5 :
class-map: COPPCLASS_OSPF (match-any)
class-map: COPPCLASS_LDP (match-any)
Earl in slot 5 :
class-map: COPPCLASS_BGP (match-any)
class-map: COPPCLASS_MISC (match-any)
class-map: COPPCLASS_UNDESIRABLE (match-any)
Earl in slot 5 :
class-map: COPPCLASS_IPV4_CATCHALL (match-any)
Earl in slot 5 :
class-map: COPPCLASS_IPV6_CATCHALL (match-any)
class-map: class-default (match-any)
Earl in slot 5 :
```

  When this issue is triggered, the following error will be seen in the logs:

```
*Dec 14 02:33:14.579: %QM-2-TCAM_BAD_LOU: Bad TCAM LOU operation in ACL
```

  This issue potentially exposes the device to a DoS vulnerability.

  Conditions: This symptom occurs under the following conditions:

  1. 7600 HA Environment.
  2. CoPP IPV6 ACL with DSCP match.
  3. Reload or Switchover.

  Workaround: There are two workarounds for this issue.

  1. Modify the CoPP Policy to remove IPV6 ACL/DSCP matching.

2. Remove and reapply the CoPP configuration as shown below:

```
lab-7609-rsp-02(config)#control-plane
lab-7609-rsp-02(config-cp)#no service-policy in COPP
lab-7609-rsp-02(config-cp)#service-policy in COPP
lab-7609-rsp-02(config-cp)#end
```

CoPP is applied to all modulues as required:

```
lab-7609-rsp-02#sh policy-map control-plane in | inc class|Earl
class-map: COPPCLASS_MCAST (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_MGMT (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_ALLOW_ICMP (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_MONITORING (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_FILEXFER (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_REMOTEACCESS (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_OSPF (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_LDP (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_BGP (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_MISC (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_UNDESIRABLE (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
```

```
Earl in slot 8 :
class-map: COPPCLASS_IPV4_CATCHALL (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: COPPCLASS_IPV6_CATCHALL (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
class-map: class-default (match-any)
Earl in slot 1 :
Earl in slot 5 :
Earl in slot 7 :
Earl in slot 8 :
```

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

- CSCum17958

  Symptom: An IOSd crash is observed during a configuration replace.

  Conditions: This symptom occurs on configuration with a port-channel interface.

  Workaround: There is no workaround.

- CSCum24565

  Symptom:

  – MPLS is being processed by the CPU instead of HW switching.

  – **rem com sw show mls vlan-ram** shows "0" value under vpn-num and netdr shows that mpls is being processed by the CPU:

```
Example: 7600# rem comm sw sh mls vlan-ram 1906 1906
TYCHO Vlan RAM Key: * => Set, - => Clear
vlan eom nf-vpn mpls mc-base siteid stats rpf vpn-num bgp-grp l2-metro rpf-pbr-ovr
----+---+------+----+-------+------+-----+---+-------+-------+--------+-----------
1906 * - * 0 0 - - 0 0 - * <<<=== vpn-num 0
```

  There is a possibility of a high CPU due to interrupts.

  Conditions: The symptom may occur on the Cisco 7600 Series Routers after an SSO is performed on PE with L2VPN in PFC VLAN mode.

  Workaround:

  1. Remove xconnect configuration from the subinterface and reconfigure it.
  2. Shut/no shut the xconnect source interface.

- CSCum61595

  Symptom: Alignment errors are observed after upgrading to Cisco IOS Release 15.2(4)M5.

```
Jan 9 19:42:59.623 GMT: %ALIGN-3-CORRECT: Alignment correction made at 0x6477F81Cz
reading 0x6BE87495 Jan 9 19:42:59.623 GMT: %ALIGN-3-TRACE: -Traceback= 0x6477F81Cz
0x647805D0z 0x6478FE70z 0x64751088z 0x64B99F4Cz 0x64B99FD4z 0x64752 284z 0x647525ACz
```

Conditions: This symptom does not occur under specific conditions.

Workaround: There is no workaround.

- CSCum65604

  Symptom: A Cisco router gets crashed.

  Conditions: This symptom occurs when shut/no shut is performed on the access interface.

  Workaround: There is no workaround.

- CSCum85813

  Symptom: Shut primary static router and secondary static is not installed automatically.

  Conditions: This symptom is seen on the sites where the BFD state of the backup static route is marked as “U” in the output of “show ip static route bfd”.

  Workaround: Reinstall the default backup static route.

- CSCum95330

  Symptom: Removing an Ethernet service instance which is a member of a bridge domain may cause the router to reload.

  Conditions: This symptom is observed when the last service instance is removed from the bridge domain and there are still members of the bridge domain which are not service instances (such as VFIs).

  Workaround: Completely unconfigure the bridge domain and reconfigure it.

- CSCun10381

  Symptom: A traffic drop was observed because labels do not get programmed.

  Conditions: This symptom occurs when scalable EoMPLS with L3VPN is configured. When notifications on atom-imps arrive, they have to get programmed.

  Workaround: Clear ip route.

  More Info: Traffic was seen to be dropped as the atom-imps could not be programmed because label entry could not be found for the atom-imps.

- CSCun11782

  Symptom: Rtfilter prefixes are sent with incorrect next-hop equal to next-hop of the default static route in GRT instead of BGP router-id.

  Conditions: This symptom occurs with a default static route present in GRT pointing, for example, to the next-hop known behind the connected interface.

  Workaround: Replace the default static route with a more specific static route or remove static and clear BGP.

- CSCun13688

  Symptom: The Cisco Catalyst 6500 Supervisor Engine 2T with CLNS routing configured crashes after **show clnbs route**.

  Conditions: This symptom occurs when CLNS routing is configured.

  Workaround: There is no workaround.

- CSCun20187

  Symptom: HSRP communication fails between two PEs (Cisco 7600 Series router) right after removing a neighbor from VFI.

Conditions: Assume that a VPLS circuit is running between more than two PEs say A,B, and C and HSRP is running between A and B. Removing VPLS peer C on either A or B would cause HSRP communication failure between A and B. This failure is not expected as data path is still available between A and B.

Workaround: Perform shut/no shut on the SVI.

- CSCun24813

  Symptom: In an HA setup, on standby reload, an active crash occurs.

  Conditions: There are a few states maintained on active for the tunnel reserved and tunnel global VLANs depending on the status of their usage (the one trying to free the VLAN).

  When the standby frees the VLAN, the state of VLAN is set to 2 on active. But in this case when the state of VLAN is set to 2, and the standby is reloaded, the active crashes .

  Workaround: There is no workaround.

  More Info: In an HA setup there are states maintained for the VLAN on active, depending on the active or standby that has freed it . There are 4 states : State 1: When the active wants to free the VLAN and is waiting for a message from the standby to free the VLAN. In this case, VLAN is put in delay list for 4 minutes.

  State 0: When VLAN is freed by the active, the state is set to 1.

  State 2 : When VLAN is freed by the standby, the state is set to 2.

  State 3 : Same as State 1 for global rsvd VLAN.

  Cases :

  Case 1: The active wants to free the VLAN, waits for a message from the standby, set the state to 1, before 4 minutes standby frees the VLAN and sends the message to active, the state is set to 0 .

  Case 2 : The active wants to free the VLAN first, set the state to 1, within 4 minutes if a message from the standby does not arrive, the state is set to 0. After 4 minutes the standby frees the VLAN and sends the message to active, and the state is set to 2 .

  Case 3: The standby wants to free the VLAN first, sends a message to the active, the state is set to 2, the active also frees it, and sets the state to 0 finally.

  Now when a peer reload is done, all the VLANs which are in delay list waiting for the standby message are to be freed. Here we check if the state of the VLAN is not 0, it is set to 0 and freed. In case 2, the state of the VLAN after it is deleted from the active and the standby is 2, so on reload an attempt to again free these VLANs is made, hence the crash.

- CSCun31021

  Symptom: A vulnerability in IKE module of Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to affect already established Security Associations (SA)..

  The vulnerability is due to a wrong handling of rogue IKE Main Mode packets. An attacker could exploit this vulnerability by sending a crafted Main Mode packet to an affected device. An exploit could allow the attacker to cause dropping of valid, established IKE Security Associations on an affected device.

  Conditions: Device configured to process IKE request that already has a number of established security associations.

  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 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

CVE ID CVE-2014-2143 has been assigned to document this issue.

Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2014-2143

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

- CSCun35055

  Symptom: The RPF is not cleared when the internal VLAN is freed by shutting down an interface with RPF configuration. This affects the new interface assigned with this internal VLAN.

  Conditions: This symptom occurs when an interface with RPF configuration is shut down.

  Workaround: Flap the RPF configuration for the new interface.

- CSCun48344

  Symptom: A config-sync failure occurs due to the **address-family ipv6 unicast vrf** command during the immediate unconfiguration and reconfiguration of VRF definition.

  Conditions: This symptom occurs with attached running configurations.

  Workaround: There is no workaround.

- CSCun58072

  Symptom: ifOutOctets goes backwards when an output drop happens on the FR subinterface. The PVC output counter also goes backwards.

  Conditions: This symptom occurs when there is an output drop on the FR subinterface.

  Workaround: There is no workaround.

- CSCun62181

  Symptom: A Cisco ASR 1002 router running Cisco IOS XE Release 3.4S crashes when recalculating PMTU.

  Conditions: The symptom occurs when the outgoing tunnel interface flaps.

  Workaround: There is no workaround.

- CSCun68542

  Symptom: CSR1000V router running XE3.11 (15.4(1)S) working as Route Reflector.

  The route-reflector is advertising prefixes with incorrect subnet masks to ibgp peers and route-reflector clients. The incorrect prefixes are not present in the bgp table of the route-reflector itself, however they do get installed in the bgp table of the router receiving the update.

  Conditions: This symptom is observed when BGP route reflector uses the additional paths feature.

  Workaround: Disable additional path feature either globally under address-family or per neighbor.

- CSCun73515

  Symptom: A router crashes due to RMON.

  Conditions: This symptom occurs on activation of an RMON event.

  Workaround: There is no workaround.

- CSCun77010

  Symptom: A router may crash after or during the execution of the **show ipv6 ospf rib** command.

  Conditions: This symptom occurs when many routes or route paths are present in the OSPFv3 rib. The OSPFv3 rib is significantly recomputed during execution of commands.

  Workaround: Limit the use of the **show ipv6 ospf rib** command.

- CSCun86087

  Symptom: In a VPLS environment, packets of some VCs are blocked in an imposition direction.

  Conditions: This symptom occurs with port channels and LAG as MPLS core-facing interface on ES+.

  Workaround: There is no workaround.

- CSCun90108

  Symptom: On CUBE there is a port leak seen for each audio+video call negotiated to audio call.

  Conditions: This symptom is observed when audio + Video M line offer answered with only audio m line.

  Workaround: Send answer with both audio m line and video, if video not supported send port 0.

- CSCun91923

  Symptom: CUBE reloads intermittently while handling SIP call forking scenario.

  Conditions: In SIP Call forking scenario, an INVITE sent from CUBE is routed to multiple SIP endpoints and multiple SIP provisional responses such as 183 Session Progress with different To tags are received.

  Workaround: There is no workaround.

- CSCun92095

  Symptom: IOS-XE running router may reload when unconfiguring BGP along with other removal operations in a scaled setup.

  Conditions: BGP is configured with 1Million+ nets and 4000 VRFs. Then the bgp instance is removed using “no router bgp <>”

  Workaround: Shut down the bgp neighbor sending big scale nets to remove the nets first from BGP and RIB. Then remove the BGP using “no router bgp <>”.

- CSCuo08759

  Symptom: With IP-FRR, VPLS traffic is dropped on a core-facing port-channel after a link flap.

  Conditions: This symptom occurs when a core-facing interface is a port-channel configured on a Cisco 7600 ES+ card.

  Workaround: Perform shut and no shut on the port-channel interface.

- CSCuo13314

  Symptom: ES+ crashes while deleting the imposition table from LC.

  Conditions: This symptom occurs while flapping the scalable EoMPLS.

  Workaround: There is no workaround.

- CSCuo15967

  Symptom: Receiving TCP RST does not trigger a BGP session down.

Conditions: This symptom occurs when BGP NSR (ha-mode SSO) is enabled. It is observed on a Cisco ASR 1001 router running the following releases:

- Cisco IOS XE Release 3.6.xS
- Cisco IOS XE Release 3.7.xS

Workaround: Disable NSR on the router as “no neighbor x.x.x.x ha-mode sso”.

- CSCuo16717

  Symptom: PPPoX brings up sessions failure with IPv6 configurations.

  Conditions: This symptom occurs when “vpdn authen-before-forward” is configured.

  Workaround: Do not configure “vpdn authen-before-forward”.

- CSCuo22184

  Symptom: The VPLS bit is not set in the flood VLAN LTL index which causes a traffic drop.

  Conditions: This symptom occurs under the following conditions:

  - Have a port-channel with member links on different NP (say NP2 and NP1) and a physical interface on the same LC and NP (say NP2) to different neighbors, say PE1 and PE2 respectively.
  - Shut down the member link of NP1.
  - Remote shut the VLAN or access interface on PE2 (reached by physical interface).
  - The V-bit is not set and this affects the traffic towards PE1 (reached by port-channel interface).

  Workaround:

  - Either no-shut the remote VLAN or AC on PE2.
  - Perform shut and no-shut the port-channel.

- CSCuo46913

  Symptom: A crash is seen causing a system reload. The crash occurs in the crypto IKMP process:

  ```
  Exception to IOS Thread: Frame pointer 0x3CEFFB58, PC = 0x164CC518
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Crypto IKMP
  ```

  Conditions: This symptom occurs after the following debug:

  ```
  debug cry condition peer subnet XXX.XXX.XXX.XXX XXX.XXX.XXX.XXX
  ```

  The exact conditions are still being investigated.

  Workaround: There is no workaround.

- CSCuo47685

  Symptom: While evaluating the Cisco IOS Release 15.3(3)S3 early release image, the following error message was observed when using the CoPP configuration given below which matches based on precedence only as shown:

  ```
  class-map match-any coppclass-protocol match precedence 6 7
  ```

  “Match precedence in IPv4/IPv6 packets is not supported for this interface error: failed to install policy map CoPP”

  Upon occurrence, the entire CoPP policy map is not loaded. There is a concern that some field devices on the current release (Cisco IOS Release 15.0(1)S6) may have the above configuration and as such is prone to this error (CoPP installation failure during upgrade).

Conditions: This symptom occurs while evaluating the Cisco IOS Release 15.3(3)S3 early release image.

Workaround: There is no workaround.

- CSCuo48507

  Symptom: While testing ISSU from XE310<->XE311 with ikev2_dvti and GRE features, packet drops is observed after a switchover.

  Conditions: This symptom is observed during upgrade to Cisco IOS Release 3.11 and downgrade to Cisco IOS Release XE 3.10.

  Workaround: There is no workaround.

- CSCuo49923

  Symptom: Performing an ISSU upgrade with the CEF table consistency checkers enabled may result in a crash on “issu runversion”.

  Conditions: This symptom occurs with a Cisco Catalyst 6500 Series Switch running Cisco IOS Release 15.1(02)SY.

  Workaround: Turn off the CEF table consistency checkers before performing an ISSU upgrade.

- CSCuo53561

  Symptom: BGP fails to apply an inbound route map on prefixes after a switch over.

  Conditions: This symptom occurs when NSR is enabled and RP switchover is performed twice.

  Workaround: Enable the knob “bgp sso route-refresh-enable” or manually do a soft refresh to get the routes back from NSR peers on the new active RP.

- CSCuo56871

  Symptom: A Cisco ASR 1001 router running Cisco IOS Release 15.2(4)S4 acting as a route server crashes when **clear bgp ipv4 unicast *** is executed.

  Conditions: This symptom occurs when a router is configured as as route server and a command executed in an IPv4 table is reset via **clear bgp ipv4 unicast ***.

  Workaround: Do not execute command **clear bgp ipv4 unicast ***. Instead, one could use the **clear ip bgp *** to hard reset all the BGP tables.

- CSCuo60001

  Symptom: MFR links do not come up.

  Conditions: This symptom occurs when SPA reloads.

  Workaround: There is no workaround.

- CSCuo62753

  Symptom: SIP400 LC microcode goes into error state.

  Conditions: This symptom occurs when FRF12 is configured and a microcode reload is done.

  Workaround: Perform an LC reload.

- CSCuo70773

  Symptom: Confidence levels sent to an ASR server from VXML gateway in the MRCPv2 messages are not the expected values. The values may appear to have had their leading zero after decimal place removed or trimmed.

  Conditions: This symptom occurs under the following conditions:

  – MRCPv2

  - Incoming confidence level in VXML document is less than 0.10

  Workaround: Do not use a confidence level value smaller than 0.10 in VXML documents. Do not provide a confidence level that has a leading zero after the decimal point. Example: 0.05.

- CSCuo76187

  Symptom: BGP peer terminates session with NOTIFICATION 3/10 (illegal network).

  Conditions: This symptom occurs when a recursively known VPNv4 route is advertised from an IOS-based router to XR or JunOS based router. The issue is not observed when both peers are running IOS.

  Workaround: There is no workaround.

- CSCuo83510

  Symptom: A stack overflow and boot loop can occur when configuring OSPFv3 for IPv6 using a non-broadcast network type on IOS XE

  Conditions: SVI or Layer-3 Interface using the ospf non-broadcast network type.

  Workaround: Remove the non-broadcast network configuration.

  Further Problem Description:This issue was found during a security audit of the product.

  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

- CSCup11582

  Symptom: A Cisco router randomly crashes.

  Conditions: This symptom occurs with normal SIP voice traffic with TLS signaling and SRTP for media flows.

  Workaround: There is no workaround.

- CSCup18062

  Symptom: A memory leak is observed.

  Conditions: This symptom occurs on a device running Cisco IOS XE Release 3.7.5S. The leak does not occur with all crypto map-related configuration. It occurs with RSA authentication and with specific configuration as shown below:

  ```
  crypto dynamic-map itcard_dynamic 600 set transform-set <name> set pfs group5 set
  identity IDENTITY600>*** match address IDENTITY600
  ```

  Workaround: There is no workaround.

- CSCup22590

  Symptom: Some Cisco Internetwork Operating System (IOS) releases may be affected by the following vulnerabilities:

  These products include a version of openssl that is affected by the vulnerabilities identified by the Common Vulnerability and Exposures (CVE) IDs:

  CVE-2014-0195 - DTLS invalid fragment vulnerability

  CVE-2014-0221 - DTLS recursion flaw

CVE-2014-0224 - SSL/TLS MITM vulnerability

This bug has been opened to address the potential impact on this product.

Conditions: Devices running an affected version of Cisco IOS and utilizing an affected configuration.

One of more of these vulnerabilities affect all versions of IOS prior to the versions listed in the Integrated In field of this defect.

Workaround: There is no workaround.

Further Problem Description: Customers may utilize the Cisco IOS Software Checker to see if their releases are impacted by these vulnerabilities.

The Cisco IOS Software Checker can be found here:
http://tools.cisco.com/security/center/selectIOSVersion.x

Customers will need to input the version(s) of IOS that are of interest in Step 1. At Step 2, customers should select “All previously published Cisco Security Advisories”. If affected by the June 5th OpenSSL Cisco Security Advisory it will be listed in the results.

CVE-2014-0224: All Cisco IOS services that provide a form of TLS or SSL encryption are affected by this vulnerability. This includes features such as the HTTPS Web Management interface.

CVE-2014-0195: Cisco IOS devices that support SSLVPN (AnyConnect) and have the feature configured and enabled are affected by this vulnerability.

CVE-2014-0221: Cisco IOS devices that support SSLVPN (AnyConnect) and have the feature configured and enabled are affected by this vulnerability.

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 10/9.5:

https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:U/RC:C

The Cisco PSIRT has assigned this score based on information obtained from multiple sources. This includes the CVSS score assigned by the third-party vendor when available. The CVSS score assigned may not reflect the actual impact on the Cisco Product.

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

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCup23792

  Symptom: A loss of service-group configuration under a subinterface is observed.

  Conditions: This symptom occurs only when the router is reloaded. It is not seen with a particular LC reload where the interface exists.

  Workaround: There is no workaround.

- CSCup53658

  Symptom: q-in-q subinterfaces on a Cisco ASR 1000 Series router do not show correct traffic statistics via SNMP ifTable/ifXTable or CLI (show vlans dot1q).

  Conditions: This symptom occurs when the subinterface is configured under a port channel. The issue is not seen when the subinterface is a part of the physical interface.

  Workaround: Traffic statistics via CLI can be obtained directly from the SPA by using the following command for each member interface of the port channel:

  Using Gi1/3/0 as an example:

  request platform software console attach 1/3

(Note: On Cisco ASR 1000 releases prior to XE 3.2 this command may fail. If so, use the hidden command: ipc-con <slot> <bay>)

```
show hw-module subslot 0 tcam all_entries vlan brief
```

Note the VLANs (denoted by V1 and V2) for which statistics are required.

```
Example: Slot-0-0>show hw-module subslot 0 tcam all_entries vlan brief ADDR PO V1 V2
C1 C2 ETYPE QVASN IPF IT IACL IRID EPF ET EACL ERID VVID PV PS DA SCTH FE RGN 2076 00
2005 1507 00 00 0000 18 2212 00 0004 0000 0002 00 0004 0000 0000 C0 00 00 0000 00 6
```

Use the following command to get VLAN TCAM statistics for the TCAM with address 2076 (that handles q-in-q for VLAN 2005 and 1507 as per V1 and V2 columns)

Output will be like the following:

```
show hw-module subslot 0 tcam counters vlan 2076 VLAN Rx Hit : Pkt: 1066 VLAN Rx
Unicast Send : Pkt: 1065 Byte: 126102 VLAN Rx Mcast Send : Pkt: 0 Byte: 0 VLAN Rx
Bcast Send : Pkt: 1 Byte: 64 VLAN Rx Osub Drop : Pkt: 0 Byte: 0 VLAN Tx Hit : Pkt:
1066 VLAN Tx Ucast Send : Pkt: 1064 Byte: 126038 VLAN Tx Mcast Send : Pkt: 0 Byte: 0
VLAN Tx Bcast Send : Pkt: 2 Byte: 128
```

Alternatively to avoid the need to look up the TCAM address beforehand, you can use the following syntax:

```
show hw-module subslot 0 tcam entry vlan 0 first-vlan-tag second-vlan-tag 0 8 8 | i
Pkt
```

The Hit counters represent overall TX/RX packet counters. The RX/TX send represent packet and byte counts for Unicast, Multicast and Broadcast Respectively

Note: The only way to clear the counters is to remove and readd the member interface from the port channel.

- CSCup66424

  Symptom: A Cisco router fails to send out any packet. The link status is up/up, but no packet is sent out the interface.

  Conditions: This symptom occurs when one interface is connected and the link status is up.

  Workaround: There is no workaround.

- CSCuq01057

  Symptom: An SP crash occurs at @tyfib_error_recovery or "%MLSCEF-SP-2-SANITY_FAIL: Sanity Check of MLS FIB s/w structures failed" is observed while performing a core interface shut/no shut with BGP PIC enabled on an L3VPN PE.

  Conditions: This symptom occurs on performing a core interface shut/no shut with BGP PIC enabled on an L3VPN PE.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S5

- CSCeh69721

  Symptom: The box crashes with the following error message:

  ```
  %SCHED-3-CORRUPT,%SCHED-3-STILLWATCHING
  ```

Conditions: This symptom occurs when the box is stress tested with e-phone calls. This is a bug at socket layer so any application which needs to duplicate a socket will encounter this sort of a bug. For example, repeated attempts for a tftp copy also can cause this.

Workaround: There is no workaround.

- CSCej00344

  Symptom: A router may reload unexpectedly when opening a terminal session.

  Conditions: This symptom can be seen on any platform. It can be seen while starting any terminal session from the router, including a mistyped command which the router by default will try to resolve as an address to telnet to. This bug is not specific to X.25 configuration and is seen when initiating an outbound telnet/ssh/rlogin session from the device. It occurs when there are multiple outbound sessions from the same terminal (console,vty).

  Workaround: There is no workaround.

- CSCsm40779

  Symptom: A router may go into initial configuration dialog on bootup.

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.4(11)T2 with the c7200p-adventerprisek9-mz image.

  Workaround: There is no workaround.

- CSCtb34814

  Symptom: The %DATACORRUPTION-1-DATAINCONSISTENCY: copy error is observed without any traceback just before the the system crashes.

  Conditions: This issue occurs under normal conditions.

  Workaround: There is no workaround.

- CSCtf31377

  Symptom: Cisco IOS crashes due to processor pool memory corruption.

  Conditions: This symptom occurs due to processor pool memory corruption. IOS generates one or more CLUE memory error messages similar to the following messages:

  ```
  %CLUE-DFC3-3-SOR_CORRUPT: CLUE record corruption in start of record field, record id
  3341, record starting address 0x5FFFFF90
  ```

  This issue could also be seen on LAN cards of a Cisco 7600 router.

  Workaround: There is no workaround.

- CSCtn04686

  Symptom: 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.

- CSCtz13023

  Symptom: A crash occurs during registration in SRST mode.

  Conditions: This symptom occurs during registration in SRST mode.

  Workaround: This issue is fixed and committed.

- CSCtz19192

  Symptom: Router crashes with the following message:

  ```
  "Unexpected exception to CPU: vector 1200".
  ```

  Conditions: This symptom occurs due to a change in the bandwidth or policing rate of the dialer interface.

  Workaround: Downgrade to Cisco IOS Release 15.1(4)M4.

- CSCtz66347

  Symptom: Router crashes on executing **show tech-support** from the linux client to the IOS server over an SSH session with the rekey enabled.

  Conditions: This symptom occurs when the rekey value “ip ssh rekey volume 400” is configured.

  Workaround: Disable the rekey feature by configuring the **no ip ssh rekey** command.

- CSCtz73473

  Symptom: In a rare multipath import configuration on IOS router, the following traceback is seen:

  ```
  SW0: *May 4 12:08:40.175 PDT: %IPRT-3-INVALID_NEXTHOP: Duplicate ID 0x3 113.1.1.0/24
  from bgp decode: 0x6770760 ---> ip_route_update+37C 0x59F7B20 --->
  bgp_ipv4_rib_install+578 0x59F87C8 ---> bgp_ipv4_rib_update+108 0x5A8C524 --->
  bgp_vpnv4_update_iprib+2C 0x59F8C24 ---> bgp_v4class_update_fwdtable_walker+60
  ```

  Though there is no operational impact, it disturbs the console with the above traceback.

  Conditions: This symptom is observed when you configure the following in the VRF address family:

  ```
  router bgp 200000
  !
  address-family ipv4 vrf 5
  import path selection multipaths
  maximum-paths eibgp 8
  ```

  Workaround: Do not log output on console but make it buffered to keep console clean.

- CSCua18166

  Symptoms: When sub appid is triggered by end points, the network does not recognize it and displays it as “Unknown identifier”.

  Conditions: This symptom occurs when the limitation results in not supporting traffic classification based on sub appid.

  Workaround: There is no workaround.

- CSCua44483

  Symptoms: Mcast stops sending for all groups once all flows have ceased, due to timeout.

  Conditions: This symptom occurs during normal operation, after senders have stopped sending and/or flows have timed out as normal.

  Workaround: Disable and reenable mcast routing.

- CSCua60785

  Symptoms: Metadata class-map matches only the first of the following filter, if present, in a class map (the other media-type matches are skipped):

  match application attribute [category, sub-category, media-type, device-class] *value-string* **match application application-group** *value-string*

  Conditions: Seen in a case where the class map has the aforementioned filters.

Workaround: There is no workaround.

- CSCua86620

  Symptoms: The vmware-view application is not detected/classified.

  Conditions: This symptom is observed when vmware-view applications are used.

  Workaround: There is no workaround.

- CSCuc18606

  Symptoms: After BGP flap or device reload, the following error is displayed in the log:

  ```
  BGP-3-DELROUTE Unable to remove route for [XYZ] from radix trie
  ```

  There is also a reachability issue.

  Conditions: This symptom is observed during BGP flap, router reload, and when changing the NET statement under the ISIS process.

  Workaround: Reconfiguring NET under ISIS or reloading the device may help to resolve the issue.

- CSCuc28931

  Symptom: The router crashes due to high CPU and lack of memory.

  Conditions: This symptom occurs when using a local connect between an EFP with encap dot1q and an EFP with encap untagged.

  Workaround: There is no workaround.

- CSCuc41531

  Symptoms: Forwarding loop is observed for some PfR-controlled traffic.

  Conditions: This symptom is observed with the following conditions:

  - Traffic Classes (TCs) are controlled via PBR.
  - The parent route is withdrawn on selected BR/exit.

  Workaround: This issue does not affect configured or statically defined applications, but only affects learned applications so this can be used as one workaround. Another option is to issue shut/no shut on PfR master or clear the related TCs with the **clear pfr master traffic-class ...** command (this fixes the issue until the next occurrence).

- CSCuc99750

  Symptom: EIGRP routes, that are not Feasible Successor are getting into the routing table.

  Conditions: This symptom is observed when you increase variance and maximum paths.

  Workaround: There is no workaround.

- CSCud63146

  Symptoms: In a GETVPN scenario, the GM fails to install policies on reload. A crypto map is applied on ethernet 0/0 while the local address of the crypto map is configured with ethernet 0/1.1

  Conditions: This symptom occurs after a reload. The GM fails to install policies from the key server.

  Workaround: Remove the crypto map configuration on the interface and reapply.

- CSCue68714

  Symptom: Newer released IOS-XE BGP, post Cisco IOS Release 15.2(4)S/XE3.7 not forming BFD session with the older implementations. This happens when using eBGP multi-hop to peer between two loopback interfaces on directly connected routers.

Conditions: This ddts adds a couple of options "[single-hop | multi-hop]" to the existing BGP-BFD knob "neighbor x.x.x.x fall-over [bfd] [check-control-plane-failure]".

So, after the change the knob would be: "neighbor x.x.x.x fall-over [bfd] [single-hop | multi-hop] [check-control-plane-failure]"

**Note: Existing: "neighbor x.x.x.x fall-over [bfd]" --- This behavior would not be disturbed; so that we do not change the behavior that has been released as part of all the releases for more than three years now.

Add-on in this ddts:

1) "neighbor x.x.x.x fall-over [bfd] [single-hop] -- NEW-option "single-hop"; would force BGP to open a single-hop bfd session. Even in case of back-to-back ebgp update-source loopback with 2 hop BGP peering.

2) "neighbor x.x.x.x fall-over [bfd] [multi-hop] -- NEW-option "multi-hop""; would force BGP to open a multi-hop bfd session.

Workaround: There is no work around. ISR G2 should support BFD multi-hop feature.

More Info: ISR-G2 does not support multi-hop BFD, while ISR4400 supports multi-hop BFD. BFD multi-hop support for ISR-G2 needs to be provided, so that they can interop with ISR4400 and ASRs.

- CSCue69214

  Symptom: Memory leaks are seen in the metadata after removing a virtual interface.

  Conditions: This symptom occurs after removing a virtual interface, if metadata is enabled.

  Workaround: There is no workaround.

- CSCue95644

  Symptom: This is the Cisco response to research performed by Mr. Philipp Schmidt and Mr. Jens Steube from the Hashcat Project on the weakness of Type 4 passwords on Cisco IOS and Cisco IOS XE devices. Mr. Schmidt and Mr. Steube reported this issue to the Cisco PSIRT on March 12, 2013.

  Cisco would like to thank Mr. Schmidt and Mr. Steube for sharing their research with Cisco and working toward a coordinated disclosure of this issue.

  A limited number of Cisco IOS and Cisco IOS XE releases based on the Cisco IOS 15 code base include support for a new algorithm to hash user-provided plaintext passwords. This algorithm is called Type 4, and a password hashed using this algorithm is referred to as a Type 4 password. The Type 4 algorithm was designed to be a stronger alternative to the existing Type 5 and Type 7 algorithms to increase the resiliency of passwords used for the enable secret password and username username secret password commands against brute-force attacks.

  This Cisco Security Response is available at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20130318-type4

  Conditions: See the published Cisco Security Response.

  Workaround: See the published Cisco Security Response.

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and a Cisco Security Response is available at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20130318-type4

  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

- CSCuf53543

  Symptom: MPLS-TP L2 VCs are down after an SIP reload and RP switchover.

  Conditions: This symptom occurs when VCs are configured through an MPLS-TP tunnel in a hardware redundant platform.

  Workaround: There is no workaround.

- CSCuf56842

  Symptom: A reload may occur while using **show oer** and **show pfr** commands via SSH.

  Conditions: This symptom is observed when the **show pfr master application detail** command is used via SSH.

  Workaround: There is no workaround.

- CSCug22238

  Symptom: UUS/UUI fields from a refer are not sent out on the corresponding INVITE when this is a SIP GW.

  Conditions: This symptom is observed in Cisco IOS Release 15.1.4M6.

  Workaround: There is no workaround.

- CSCug43009

  Symptom: SYS-SP-2-MALLOCFAIL memory allocation fails due to I/O buffer memory leak in process_online_diag_pak.

  Conditions: This symptom occurs when some diag packets get en-queued to a queue which is not being watched. Hence, there is no dequeueing on that queue which leads to I/O memory leak.

  Workaround: Reload the box to clear the I/O pool when it is full.

- CSCug50606

  Symptom: Sometimes, IPCP assigns an different address for clients from wrong address pool.

  Conditions: This symptom is observed under the following conditions:

  - **peer default ip address** command is configured on dialers.
  - There are some dialers on the Cisco router.
  - The issue could happen on Cisco IOS Release 15.2(4)M3.

  Workaround: There is no workaround.

- CSCug71297

  Symptom: An SP crash is observed at the below RPC call block during an ISSU upgrade after commit version.

  ```
  SP: Frames of RPC pf_issu_sp2rp process (pid 579) on 16 (proc|slot) after blocking rpc
  call failed: 42342B84
  ```

  Conditions: This symptom occurs during ISSU commit version while saving the configuration.

  Workaround: There is no workaround.

- CSCug75194

  Symptom: A latency issue is observed. The order of packets changes.

  Conditions: This symptom occurs on EVC xconnect for MACsec packets and data packets.

  Workaround: Stop the control traffic from the peer side and send only data traffic.

- CSCug97383

  Symptom: Switch crashes with EOAM and IP SLA Ethernet-monitor configurations.

  Conditions: This issue occurs infrequently when EOAM configuration include VLANs. Does not occur if all EOAM configurations are configured with only Ethernet Virtual Circuits (EVC).

  Workaround: There is no workaround.

- CSCug99771

  Symptom: The OSPF N2 default route is missing from the spoke upon reloading the hub. The hub has a static default route configured and sends that route over the DMVPN tunnel running OSPF to spoke. When the hub is reloaded, the default route is missing on the spoke. NSSA-External LSA is present on the spoke after reload, but the routing bit is not set. Hence, it is not installed in RIB on the spoke.

  Conditions: Default originated using the **area X nssa default-information-originate** command.

  Workaround: Removing & readding **area X nssa default-information-originate** on the hub resolves the issue.

- CSCuh09324

  Symptom: UDP-based entries are not deleted from the flowmgr table resulting in a crash or poor system response with CPU hog messages being shown.

  Conditions: This symptom occurs in ct5760-ipservicesk9.bin cat3k_caa-universalk9.bin and cat4500e-universalk9.bin images

  The device is configured with UDP services that originate from the device. This includes but not limited to the following features:

  - TFTP
  - Energy Wise
  - DNS
  - Cisco TrustSec

  Workaround: Enter the following commands:

```
Router#config terminal
service internal
end
Router#show flowmgr
```

  The output of this command will show many lines entries holding with the same port numbers. Disabling the feature that is being held in the flows until an upgrade can be performed, is a workaround.

  A reload is required to clear the held flows.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2013-6704 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at: http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-6704

  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

- CSCuh37664

  Symptom: Prefixes/TCs stay INPOLICY although some configured resolvers are above threshold.

  Conditions: This symptom is observed when the policy uses non-default resolvers.

  Workaround: Reload the MC.

- CSCuh41290

  Symptom: After the unavailability of the LDAP CRL, no new CRL fetches can be done because LDAP waits for a reply infinitely and never times out.

  Conditions: This symptom was first seen on Cisco IOS Release 15.1(4)M6 but is not exclusive to it.

  Workaround: Set “revocation-check none” under affected trustpoint. Reload router.

- CSCuh45042

  Symptom: Traffic on some GIG subinterfaces are seen to be dropped at the SPA. The SPA TCAM is seen to have two entries sharing the same logical address as a result of which one entry is seen to overwrite the other.

  Conditions: This symptom was observed after a router/LC/SPA reload. The exact condition that triggers this symptom is not known.

  Workaround: There is no workaround.

- CSCuh69292

  Symptom: LDAP moves in the stuck state.

  Conditions: This issue is seen if the LDAP server becomes unavailable during LDAP transactions.

  Workaround: There is no workaround.

- CSCuh91645

  Symptom: WS-SUP720-3B crashes while receiving DHCP packets.

  Conditions: This symptom occurs with the **ip dhcp relay information policy-action encapsulate** command.

  Workaround 1. Use the **ip dhcp relay information policy-action replace** command.

  Workaround 2. Use the **no ip dhcp relay information trusted** command.

- CSCuh94035

  Symptom: A watchdog timeout crash occurs.

  Conditions: This symptom occurs when IPv4 or IPv6 EIGRP are configured. A crash occurs while DUAL is updating the EIGRP topology table.

  Workaround: There is no workaround.

- CSCuh97129

  Symptom: Losing EIGRP Extended communities on BGP L3VPN route.

  Conditions: This symptom is observed when Remote PE-CE connection is brought down and only backup EIGRP path remains in the BGP table.

  Workaround: Clearing the problem route in the VRF will resolve the issue.

- CSCui04530

  Symptom: Upon FPD upgrade, you get this error on Cisco IOS c7600 switch:

```
! %FPD_MGMT-3-BUNDLE_EXTRACT_ERROR: Cannot extract the ssc-600-fpd.bndl bundle from
sup-bootdisk:c7600-fpd-pkg.151kg - The required bundle is not in the package file.
Please make sure that you have the right FPD image package file. % Cannot get the
required data from the indicated file, please verify that you have a valid file and
entered a valid URL. !
```

Conditions: This symptom is observed under the following conditions:

```
IOS: c7600s72033-advipservicesk9-mz.122-33.SRB3
CARDS: WS-SSC-600 WS-IPSEC-3
CLI: upgrade hw-module slot x fpd file sup-bootdisk:c7600-fpd-pkg.151-3.S2.pkg
```

Workaround: Upgrade to FPD image that includes corresponding *.bndl image.

- CSCui14692

  Symptom: Crash on C819G running 152-4.M1 due to memory corruption at vm_xif_malloc_bounded_stub.

  Conditions: This condition is seen due to recursive function call of fib code, NHRP, IP SLA etc. However, these might not be the only trigger.

  Workaround: There is no workaround.

- CSCui17064

  Symptom: A traffic drop is seen while sending traffic from CE to PE.

  Conditions: This symptom is observed if l2acl is configured in PE to permit broadcast and multicast traffic. While sending traffic from CE to PE, packets are dropped.

  Workaround: There is no workaround.

- CSCui21030

  Symptom: A vulnerability in OSPF implementation of Cisco IOS and Cisco IOS XE could allow an unauthenticated, adjacent attacker to cause a reload of the affected device.

  The vulnerability is due to improper parsing of certain options in OSPF LSA type 11 packets. An attacker could exploit this vulnerability by sending LSA type 11 OSPF packet with unusual options set. An exploit could allow the attacker to cause a reload of the affected device.

  Conditions: This symptom occurs on receiving a bad RI opaque LSA with some unusual options.

  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 5.7/4.7:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2013-5527 has been assigned to document this issue.

  Additional details about the vulnerability described here can be found at:
  http://tools.cisco.com/security/center/content/CiscoSecurityNotice/CVE-2013-5527

  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

- CSCui34165

  Symptom: Port-channel QoS features might fail to work after a router reload, followed by QoS configuration modification.

  Conditions: This symptom occurs when a vlan load-balanced port-channel is used with policy aggregation configuration where the QoS policy is configured on member links and the port-channel sub-interface, and after a system reload (configuration is from startup config).

Workaround: Reload the router without port-channel QoS configuration, and add port-channel QoS configuration to the running configuration after the router boots up.

- CSCui46593

  Symptom: CPU hog crash due to Mwheel Process.

  Conditions: This symptom is observed in a normal operation.

  Workaround: There is no workaround.

- CSCui59185

  Symptom: ASR901 crashes while booting up with memory lite disabled.

  Conditions: This symptom is observed when RFLA is enabled with memory lite disabled.

  Workaround: Enable memory lite.

- CSCui65083

  Symptom: CoS Markings are not being preserved on the dot1q interface after reload.

  Conditions: This symptom occurs under the following conditions:

  1. Policy Map (with “match cos”) applied on the main interface with the subinterface as dot1q.
  2. Reload the router.

  Workaround: Unconfigure the service-policy from interface and configure it again.

- CSCui65914

  Symptom: Minor or major temperature alarms are reported in the syslog along with the following DATACORRUPTION logs:

  ```
  Aug 5 15:54:30.972 Buc: DATACORRUPTION-SP-1-DATAINCONSISTENCY copy error, -PC=
  0x414DEED4z -Traceback= 4027C4F4 419551C0 414DEED4 414E5BC4 414E0CA0 414E0F00 Aug 5
  15:54:30.972 Buc: C6KENV-SP-4-MINORTEMPALARM interface 10/0 outlet temperature crossed
  threshold #1(=60C). It has exceeded normal operating temperature range.
  ```

  Conditions: This symptom is observed on ES+ series linecards of Cisco 7600 Series Routers.

  Workaround: There is no workaround.

- CSCui67919

  Symptom: QoS policy applied on AToM SVI does not get any matches until the user removes and reapplies the policy. Once the policy is reapplied, the policy works as expected. However, the QoS counters do not get updated and the policy statistics cannot be verified with “show policy-map interface x/x”.

  Conditions: This symptom is observed when the xconnect is applied under SVI and the core facing line card is ES20 running Cisco IOS Release 15.2(4)S3a.

  Workaround: Reapply the policy. Please note that QoS counters in “show policy-map interface xx” will not work but the policy comes in effect after re-applying it.

- CSCui74609

  Symptom: After a RSP switchover the backup pseudowire state is down and never recovers to standby state.

  Conditions: This symptom occurs on CEM circuits in an SAToP environment after an SSO switchover.

  Workaround: There is no workaround.

- CSCui76564

  Symptom: A roaming mobile customer (example: iPASS, Boingo etc.) logs on via a Web-Portal-Page and the ISG doesn't send in the radius accounting-request packet from the V-Cookie to the Radius Server.

  Conditions: This symptom occurs depending on the ISG setup. In this case L & V Cookie must be sent in accounting-request from the ISG to the AAA Server.

  Workaround: There is no workaround.

- CSCui82757

  Symptom: Session query responses in lite sessions have inconsistent calling-station-ID behavior.

  Conditions: This symptom occurs when:

  1. Walkby feature is enabled with L4R & PBHK features applied to lite session.
  2. Session query is sent to ISG.

  Workaround: Do not use calling-station-ID.

- CSCui82817

  Symptom: A tunnel with lower absolute metric is not advertised properly.

  Conditions: This symptom occurs under the following conditions:

  1. When there are multiple tunnels to a destination.
  2. The tunnel with a better metric comes up.
  3. When ISIS is used as IGP and both L1 and L2 are present and configured for TE.

  Workaround: Clear the ISIS sessions.

- CSCui83823

  Symptom: When CU executes show tech or any show commands which gives a long output using putty the SSH2 putty closes prematurely.

  Conditions: This symptom is observed when "term length 0" is enabled, the putty session closes prematurely while executing show tech show memory.

  Workaround: Redirect the output to a file.

- CSCui85019

  Symptom: When the command **show xconnect** is entered, it may result in a memory leak. This can be observed by entering the command **show memory debug leaks chunks** and seeing entries like this:

```
router#show memory debug leaks chunks
Adding blocks for GD...
I/O memory
Address Size Alloc_pc PID Alloc-Proc Name
Chunk Elements:
AllocPC Address Size Parent Name
Processor memory
Address Size Alloc_pc PID Alloc-Proc Name
AA3F8B4 2348 6D0B528 97 Exec
PW/UDP VC event trace
```

  Conditions: This symptom is observed when one or more xconnects are configured with UDP encapsulation.

  Workaround: There is no workaround.

- CSCui89069

  Symptom: An ISIS flap is observed on performing SSO.

  Conditions: This symptom occurs when **nsf ietf** is configured and one or more loopbacks are configured as passive interfaces.

  Workaround 1. Use **nsf cisco**.

  Workaround 2. Continue to use **nsf ietf** but configure **ip router isis <process_name>** on the loopback interfaces.

- CSCui90811

  Symptom: While running the Cisco IOS 15.3S release and Cisco IOS 15.4S release software for the L2VPN pseudowire redundancy feature on a Cisco router, the traffic is dropped when the primary pseudowire becomes active.

  Conditions: Initially the primary pseudowire is down due to either a local or a remote core-facing interface being shutdown. The backup pseudowire is active and traffic flows through the backup pseudowire. Later, when the backup pseudowire is down, the primary pseudowire is brought up and becomes active and traffic is not able to flow through primary pseudowire and is dropped.

  Workaround: There is no workaround.

- CSCui99031

  Symptom: In a pair of Cisco 7609-S routers running c7600rsp72043-advipservicesk9-mz.151-3.S5.bin IOS, phase 1 fails to establish due to a “signature invalid!” error when rsa-sig is used for phase 1 authentication.

  Conditions: This symptom occurs under the following conditions:

  - rsa-sig is used for phase 1 authentication
  - site to site tunnel

  Workaround: Use PSK instead of PKI.

- CSCuj00746

  Symptom: On performing an upgrade from 9.512 to 9.523, there is a label allocation failure in VPWS circuits as they are trying to utilize the labels that are already used by the VPLS circuits that are present in the database.

  Conditions: This symptom occurs when both VPWS and VPLS circuits are configured on the same node before upgrading.

  Workaround: Removing the VPLS circuit brings up the VPWS circuits. Reconfiguring the VPLS circuit is also successful with a different local label assigned.

- CSCuj11232

  Symptom: Changing the local label on an existing static (no signaling) Any Transport over MPLS (AToM) pseudowire, or changing the static pseudowire to a dynamic one (with LDP signaling) may cause traffic to fail to traverse the pseudowire.

  Conditions: This symptom is observed when either the configured value of the static local label is changed, or if the pseudowire is changed to a dynamic one.

  Workaround: Completely unconfigure the existing xconnect or pseudowire before entering the new configuration.

- CSCuj11576

  Symptom: A router experiences a crash when BFD is configured.

  Conditions: This symptom occurs when BFD is configured.

Workaround: There is no workaround.

- CSCuj16742

  Symptom: In a pseudowire redundancy configuration, packets may fail to flow even though the xconnect virtual circuit appears to be up.

  Conditions: This symptom has been observed when the xconnect is re-provisioned while the primary pseudowire is down and the backup pseudowire is up. The issue has only been observed on Circuit Emulation (CEM) attachment circuits, but it is possible other attachment circuit types may be affected as well.

  Workaround: Completely unconfigure the xconnect and then reconfigure it.

- CSCuj17482

  Symptom: On a device running low on memory, an EFP is attempted to be deleted, but fails due to lack of memory. The second attempt at removing that same EFP causes the router to restart.

  Conditions: This symptom occurs when the a lot of configuration has been applied to the device, causing high memory usage.

  Workaround: Do not overconfigure the device.

- CSCuj22189

  Symptom: On a Cisco ASR series router, a crash occurs when **mpls ip** is added under the interface.

  Conditions: This symptom occurs when the hidden command **snmp-server hc poll** is already configured.

  Workaround: Ensure that the hidden command **snmp-server hc poll** has not been configured.

- CSCuj26593

  Symptom: Simple IP Dual stack and IPv6 sessions failed to survive an RP switchover.

  Conditions: This symptom occurs when the dual stack session exists.

  Workaround: Do not use the dual stack session.

- CSCuj30702

  Symptom: This bug is specific to port channel sub interface configuration in ES+ card. This bug is not relevant to any other port channel configuration in ES+, that is, EVC/Bridge-Domain over PoCH sub-int etc, and other card types, such as ES20/ LAN cards are free from this bug. Any type of IP communication on port channel sub interfaces in ES+ cards fail. Such an issue is seen only with port channel sub interfaces on ES+ and not seen with port channel main interfaces.

  Conditions: This symptom will only be seen with images where the fix of CSCuh40617 is integrated.

  Workaround: The connections will work fine if it is moved to the main interface or by using EVC BD configurations.

- CSCuj31090

  Symptom: When L2TPv3-based pseudowire is configured between two PE routers and different VLAN ids are used on the ACs on both sides, ES+ on egress PE does not rewrite a dot1q VLAN tag when sending a frame toward CE.

  Conditions: This symptom occurs when:

  1. Both ACs are Ethernet VLAN type.
  2. Different dot1q tag is used on both ACs.

  Workaround: Configure the same dot1q tag for the ACs on both PEs.

- CSCuj39400

  Symptom: A Cisco 3945 series router running Cisco IOS Release 15.2(2)T2 may crash with a bus error. This relates to VOIP_RTCP.

  Conditions: This symprom has been observed to occur often while running SIP debugs. However, at least one identical crash happened after SIP debugs were disabled three days before.

  Workaround: There is no known workaround.

- CSCuj47554

  Symptom: PBHK bundles are not released even after the session is cleared.

  Conditions: This symptom occurs after the session is cleared and the port-bundle status is not shown correctly with **show ip portbundle status** command.

  Workaround: There is no workaround.

- CSCuj52396

  Symptom: In a VPLS Inter-Autonomous System Option B configuration, the virtual circuits between the Autonomous System Border Router (ASBR) and the PE may fail to come up.

  Conditions: This symptom is observed while initially establishing VCs after the ASBR has reloaded.

  Workaround: The **clear xconnect** exec command can be used to clear the VCs that are down.

- CSCuj57367

  Symptom: A 10 gig line card crashes on a Cisco 7600 platform with the following or similar errors:

  ```
  %SYS-DFC3-3-MGDTIMER: Uninitialized timer, timer stop, timer = 30CCCFB0. -Process= "RO
  Notify Timers", ipl= 0, pid= 7 -Traceback= 2060E1BCz 2060E8E4z %SYS-DFC3-3-MGDTIMER:
  Uninitialized timer, timer stop, timer = 30CCD154. -Process= "RO Notify Timers", ipl=
  0, pid= 7 -Traceback= 2060E1BCz 2060E8E4z %SYS-DFC3-3-MGDTIMER: Uninitialized timer,
  timer stop, timer = 30CCCFB0. -Process= "RO Notify Timers", ipl= 0, pid= 7 -Traceback=
  2060E1BCz 2060E8E4z
  08:54:43 Central Tue Oct 1 2013: Address Error (load or instruction fetch) exception,
  CPU signal 10, PC = 0x20642A08
  ```

  Conditions: This symptom occurs when a large number of IPC messages are used.

  Workaround: There is no workaround.

  More Info: On mac-scaling, the L2-DRV application sends more ICC messages(though not always). But periodically(approximately 2-3 minutes), some burst of around 150 ICC messages are sent by the SP towards the RP. This means that mac-scaling has a direct correlation with the number of IPC messages being sent.

- CSCuj58299

  Symptom: Interface input queue starts to become congested. The input queue can reach the input queue maximum which will cause problems for all control-plane and punted traffic (management, routing protocols, call control, etc).

  Example from the **show interface** output:

  ```
  Input queue: 76/75/0/5549 (size/max/drops/flushes); Total output drops: 0
  ```

  It may seem like the router becomes “unresponsive” and may require a reboot to restore service. Access from the console will still be possible. After some time, the input queue can clear on its own.

  Conditions: This symptom is observed under the following conditions:

  1. Router serves as a SIP-SIP CUBE

2. Packets that are congesting input queue are RTCP packets. Check "show buffers input-interface [interface] packet". (RTCP packets are most commonly odd source/destination UDP ports in the range 16384 - 32768)
3. CUBE receives a 180 without SDP followed by a 180 with SDP on one of the call legs (collect 'debug ccsip message' for a period of time leading up to and including when you see the input queue begin to fill)

Workaround: Perform the following workaround:

1. Increase input hold-queue to a very large value.
2. Create an ACL to block RTCP traffic on interfaces (not possible if RTCP is used for inactivity detection).
3. Influence downstream call flows such that CUBE does not receive 180 without SDP followed by a 180 with SDP.

- CSCuj60533

  Symptom: Repeated CPUHOG messages may be seen along with a crash when "reload" is issued just after a bootup.

  Conditions: This symptom occurs when the line cards are still booting up and are in other states.

  Workaround: Issue "reload" after the line cards have booted.

- CSCuj65057

  Symptom: The **ip vrf forwarding** command under "aaa" is deleted after reloading the stack master.

  Conditions: This symptom occurs after reloading the stack master switch.

```
aaa new-model
!
aaa group server tacacs+ TACACS+
ip vrf forwarding VRF01
!
ip vrf VRF01
rd x.x.x.x ---------
```

  Workaround: Use the **vrf definition** command instead of the **ip vrf command to define vrf**. (This command is supported on Cisco IOS Release 12.2(58)SE or later releases.)

- CSCuj66352

  Symptom: A system crash is observed in the SNMP engine.

  Conditions: This symptom occurs under the following conditions:

  – ?show subscriber session?
  – polling the ISG-MIB
  – clearing the subscriber

  Workaround: Do not use SNMP polling.

- CSCuj68932

  Symptom: L2TPv3 tunnel with digest fails to establish. Cisco IOS device gives the following messages when "debug l2tp all" and "debug l2tp packet detail" are enabled:

```
L2TP _____:________: ERROR: SCCRQ AVP 59, vendor 0: unknown L2TP _____:________:
Unknown IETF AVP 59 in CM SCCRQ
```

Conditions: This issue is observed when IOS device peers with non-IOS device that sends IETF L2TPv3 digest AVP (IETF AVP 59) in L2TP control message. This issue is present in S images starting from Cisco IOS Release 12.2(33)XNC and in T train from Cisco IOS Release 15.3(2)T.

Workaround: There is no workaround.

- CSCuj75952

  Symptom: The Cisco ASR 1000 route processor reloads.

  Conditions: This symptom occurs during PPPoA session establishment if CAC determines that resources are low and HW-assisted CAC needs to be enabled. The router is used to terminate PPPoA sessions and Call Admission Control (CAC) is enabled.

  Workaround: Disable Call Admission Control.

- CSCuj78636

  Symptom: A memory leak is observed in the IP Switching segment.

  Conditions: This symptom occurs if a subscriber roams with the same MAC address but a different IP address . This happens only for L2 roaming and not for L3 roaming.

  Workaround: There is no workaround.

- CSCuj88523

  Symptom: In a pseudowire redundancy configuration, traffic may fail to flow after a switchover to a backup pseudowire.

  Conditions: This symptom occurs on the Cisco 7600 series routers.

  Workaround: Execute the following commands on the attachment circuit interface:

  - **shutdown**
  - **no shutdown**

- CSCuj96893

  Symptom: Cisco router hangs and it stopped passing the traffic. Customer needs to reload the router to make it work until it hangs next time. It hangs sometimes once in month.

  Conditions: This issue is seen with more than one router.

  Workaround: There is no workaround.

- CSCuj99537

  Symptom: Not all LI streams that are properly configured via SNMPv3 and appropriate ACLs and are programmed in TCAM, are intercepted and forwarded towards MD.

  Conditions: This symptom occurs in an SIP-400 based LI.

  Workaround: Remove and reapply the problematic tap but it doesn't prevent the problem from reoccurring if new LI taps are applied via SNMPv3

- CSCuj99819

  Symptom: MVPN GRE tunnels are not established.

  Conditions: BGP has a VPN peer configured using an update-source that does not have PIM enabled.

  Workaround: There is no workaround.

- CSCul11995

  Symptom: An L2TPv3 session fails to establish and Cisco IOS receives a StopCCN message from the peer with the following message in response to its ICRP message:

  ```
  "No handler for attr 68 (68)"
  ```

Conditions: This symptom occurs when IOS device peers with non-IOS devices send IETF L2TPv3 Pseudowire Type AVP (IETF AVP 68) in an ICRP message.

Workaround: There is no workaround.

- CSCul14571

  Symptom: A Cisco router can crash after OSPFv3 is unconfigured from an interface.

  Conditions: This symptom is observed when NSR is enabled.

  Workaround: Unconfigure NSR before unconfiguring OSPFv3 from an interface.

  More Info: This is extremely rare issue; the OSPFv3 should be in a process of checkpointing LSA from primary RP to standby while an interface from which the LSA was received is unconfigured.

- CSCul24682

  Symptom: L2TP LNS puts a non-negotiated magic number to LCP packets. The PPPoE client may terminate the session prematurely due to the unknown magic number.

  Conditions: This symptom occurs when L2TP LAC does not negotiate the magic number with the PPPoE client and L2TP LNS does not renegotiate options with the PPPoE client.

  Workaround: Configure “lcp renegotiation always” on L2TP LNS.

- CSCul27327

  Symptom: On the Cisco c7600 router, if PIM is configured on the port-channel and on the port members, any failure on one of the port members will disable the FE CAM.

  Conditions: This symptom occurs when PIM is configured on the port members.

  Workaround:

  1. Do not configure PIM sparse-mode on the port members even though the CLI is accepted.
  2. In case the PIM sparse-mode is configured on the port members, remove it from the port members and the port-channel and then reapply the PIM configuration on the port-channel only.

  Further Problem Description: A similar issue (CSCtf75608) is seen on the Cisco Catalyst 6500 Series Switches, but the workaround is to configure PIM on the port-channel and the port members to avert the FE CAM to be disabled in the event of one of the port members failing.

- CSCul40898

  Symptom: After reloading the router or fresh service-instance configuration, traffic received from the access is sent to the core without a dummy VLAN header. This traffic is received by a remote PE2 and sent to switch with a missing VLAN header. Therefore CE2 drops received packets. When the issue is removed, captured traffic in the core contains a dummy VLAN header.

  Conditions: This symptom is occasionally observed when the router is reloaded and is consistently observed when a new service instance is configured as an xconnect member.

  Workaround: Perform **shutdown** followed by **no shutdown** on the service instance.

- CSCul47135

  Symptom: On Cisco ASR 1000 routers, services are not removed or applied from the active subscriber sessions when CoA is sent from the radius server. The router sends wrong values in response to the CoA request packet.

  Conditions: This symptom occurs when 15.2(20130918:081157) is run.

  Workaround: There is no workaround.

- CSCul54254

  Symptom: Invalid LSAs are not flushed by the router which has their Advertising Router ID. Specifically, Router LSAs which do not have LSID of 0 will not be flushed if the router does not re-originate them, and any LSA with a type that the router does not recognize.

  Lingering LSAs could lead to incorrect routing in some very obscure instances. For example, stale Router LSA fragments from two neighboring routers would need to remain in the network. There would not be a routing problem if only one router's stale Router LSA fragment was allowed to linger.

  Conditions: There are several possible scenarios that could lead to this symptom. One example is that a router is configured with many interfaces attached to an OSPFv3 instance such that it originates more than one Router LSA fragment. Then the router is reloaded before the configuration is saved, and after the reload it does not reoriginate some of the Router LSA fragments.

  Workaround: There is no workaround.

- CSCul65614

  Symptom: The FAN-MOD-6SHS module consumes more power than expected(should be around 180W).

```
#sh power
<SNIP>
Fan Type Watts A @42V State
---- ------------------ ------- ------ -----
1 FAN-MOD-6SHS 427.14 10.17 OK
```

  Conditions: This symptom occurs when the ES+ Combo card is placed in slot-1 of 7600 chassis.

  Workaround: Place ES+ Combo cards in any other slot other than slot-1 of 7600 chassis.

- CSCul86211

  Symptom: When LNS switches off while the sessions keep on establishing at LAC, LAC finds the l2tp db memory exhausted after sometime. Due to this, it fails to update the session in the database and during this period a crash is observed.

  Conditions: This symptom occurs when LAC tries to add l2tp session in the database and fails to do so. In order to handle this error condition, LAC frees the l2tp and l2x session twice. This double free is the reason for crash.

  Workaround: There is no workaround.

- CSCul87037

  Symptom: An "sg subrte conte" chunk leak occurs while roaming.

  Conditions: This symptom occurs after an account-logoff and if service permit is configured in control policy. In case of a service permit, the subscriber remains unauth and is redirected to the portal once again. Post successful second account logon and the subscriber session is cleared by timeout or cli, the leak is seen and the same client will not be able to create the session once again. The leak is seen after simulating for the second time account-logon. And if service permit is configured.

  In case of service disconnect configured under account-logoff, account-logon is not a practical scenario as the portal is not reachable for the client.

  Workaround: Use **service disconnect** for **event account-logoff**.

```
class type control always event account-logoff
1 service disconnect delay 10
!
```

- CSCul92497

  Symptom: The Cisco 7600 router providing layer2 EoMPLS services may stop forwarding ingress and egress traffic for an xconnect for which a backup peer config has been applied.

  Conditions: This symptom occurs in Cisco 7600 routers running Cisco IOS Release 15.2(4)S4a with ES+ cards (access/core facing) and xconnect configured under a service instance.

  Workaround: Clear the xconnect on the Cisco 7600 router side. Clearing on the remote size does not have an effect.

- CSCum65501

  Symptom: IPv6 CoPP ACL in PI matches traffic incorrectly for sw-switched paks. Packets are not hit against IPv6 ACE matching on L4 protocol. This causes traffic to be classified incorrectly.

  Conditions: This symptom occurs with recent Cisco IOS images. Results are as expected on Cisco IOS Release 12.2(33)SRE9a. However, it is broken in Cisco IOS Release 15.2(4)S4a onwards.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S4a

Cisco IOS Release 15.2(4)S4a is a rebuild release that addresses a critical issue impacting 7600 platform for Cisco IOS Release 15.2(4)S.

- CSCuj30702

  Symptom: This bug is specific to port channel sub interface configuration in ES+ card. This bug is not relevant to any other port channel configuration in ES+, that is, EVC/Bridge-Domain over PoCH sub-int etc, and other card types, such as ES20/ LAN cards are free from this bug. Any type of IP communication on port channel sub interfaces in ES+ cards fail. Such an issue is seen only with port channel sub interfaces on ES+ and not seen with port channel main interfaces.

  Conditions: This symptom will only be seen with images where the fix of CSCuh40617 is integrated.

  Workaround: The connections will work fine if it is moved to the main interface or by using EVC BD configurations.

Resolved Caveats—Cisco IOS Release 15.2(4)S4

Cisco IOS Release 15.2(4)S4 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveats in this section are resolved in Cisco IOS Release 15.2(4)S4 but may be open in previous Cisco IOS releases.

- CSCsv74508

  Symptom: If a linecard is reset (either due to an error or a command such as hw-module slot reload) at the precise time an SNMP query is trying to communicate with that linecard, the RP could reset due to a CPU vector 400 error.

  Conditions: This symptom occurs when the linecard is reset(either due to error or a command such as hw-module slot reload) at the precise time an SNMP query is received.

  Workaround: There is no workaround.

- CSCtd45679

  Symptom: The standby supervisor reloads after removing an IPSLA probe via CLI:

  ```
  R7600(config)#no ip sla 1 R7600(config)# 06:53:31: Config Sync: Line-by-Line sync
  verifying failure on command: no ip sla 1 due to parser return error
  ```

```
06:53:31: rf_reload_peer_stub: RP sending reload request to Standby. User:
Config-Sync, Reason: Configuration mismatch R7600(config)# 06:53:31:
%RF-SP-5-RF_RELOAD: Peer reload. Reason: Proxy request to reload peer R7600(config)#
06:53:31: %OIR-SP-3-PWRCYCLE: Card in module 6, is being power-cycled (RF request)
R7600(config)# 06:53:32: %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded,
changing to Simplex mode R7600(config)#
```

Conditions: This issue only occurs if the probe is configured via SNMP.

Workaround: Remove the probe via SNMP.

More Info: This issue is applicable to a Cisco Catalyst 6500 platform running Cisco IOS 12.2SX releases. It may also affect other high availability (HA) platforms running Cisco IOS 12.2 or 15.X releases.

- 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.

- CSCtr88785

  Symptoms: Following an upgrade from Cisco IOS Release 12.4(24)T2 to Cisco IOS Release 15.1(4)M1, crashes were experienced in PKI functions.

  Conditions: This symptom is observed on a Cisco 3845 running the c3845-advipservicesk9-mz.151-4.M1 image with a PKI certificate server configuration.

  Workaround: Disable Auto-enroll on the CA/RA. Manually enroll when needed.

- CSCts63581

  Symptoms: The standby PRE4 resets after write memory command at “Failed to sync private-config to standby RP”.

  Conditions: The symptom is observed with a scaled configuration that is more than NVRAM can store.

  This may occur when the standby NVRAM is locked by some other process and when config sync tries to access the standby NVRAM it fails. It then restarts the standby.

  Workaround: Significantly decrease configuration size, if possible.

- CSCtx99353

  Symptom: %SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level.

  Conditions: The symptom is observed when music on hold (MOH) is enabled.

  Workaround:

  1. Remove the route list from the multicast MOH CLI, so that you can still have music on hold and can continue the feature.
  2. Disable the MOH (but no music comes on hold).

- CSCty26035

  Symptom:

  1. There is a discrepancy in the inbound and the outbound SA lifetime in the standby router.
  2. The KB lifetime in a standby router is greater than that of the active router, when a KB lifetime rekey occurs.

3. The ping will not go through after applying a dynamic crypto map.

Conditions: The issues are seen after establishing the session between the HA routers and various test conditions.

Workaround: There is no workaround.

- CSCty59423

  Symptoms: Memory leak seen with following messages:

  ```
  Alternate Pool: None Free: 0 Cause: No Alternate pool -Process= "VOIP_RTCP", ipl= 0,
  pid= 299 -Traceback= 0x25B1F0Cz 0x25AB6CBz 0x25B1029z 0x46C02Ez 0x46C89Bz 0x46BCC2z
  0x471D12z 0x43EF59Ez 0x43DD559z 0x43DCF90z %SYS-2-MALLOCFAIL: Memory allocation of 780
  bytes failed from 0x46C02E, alignment 32
  ```

  Conditions: The conditions are unknown.

  Workaround: There is no workaround.

- CSCty77441

  Symptom: Memory leaks are observed after unconfiguring BFD sessions.

  Conditions: This symptom occurs after BFD sessions are unconfigured.

  Workaround: There is no workaround.

- CSCtz90697

  Symptoms: EIGRP authentication is not working.

  Conditions: The symptom is observed when authentication is configured with key-id 0.

  Workaround: Use any other key-id for authentication.

- CSCua21049

  Symptom: User configures a recursive multicast-only IPv6 static route. Although the static route next-hop apparently resolves in the context of the ipv6 multicast-unicast routing table, the route is not inserted in the routing table.

  Conditions: This symptom occurs when a user has configured IPv6 multicast. User has configured a recursive multicast-only ipv6 static route.

  For example:

  A user has configured recursive multicast-only static:

  ```
  ipv6 route 2001:DB8:11::1/128 2001:DB8:16::1 multicast
  ```

  Next-hop apparently resolves in context of the multicast-unicast routing table:

  ```
  rtr> show ipv6 routing multicast IPv6 Multicast Routing Table - default - 8 entries
  Codes: C - Connected, L - Local, S - Static, U - Per-user Static route B - BGP, R -
  RIP, H - NHRP, I1 - ISIS L1 I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D -
  EIGRP EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination NDr -
  Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1 OE2 - OSPF ext 2, ON1 -
  OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 ls - LISP site, ld - LISP dyn-EID C
  2001:DB8:16::/112 [0/0] via Ethernet0/1, directly connected
  ```

  However, the static route is not present in routing table and “show ipv6 static multicast detail” shows the route resolves outside the table:

  ```
  rtr> show ipv6 static multicast detail IPv6 Static routes Table - default Codes: * -
  installed in RIB, u/m - Unicast/Multicast only U - Per-user Static route N - ND Static
  route M - MIP Static route P - DHCP-PD Static route R - RHI Static route m
  2001:DB8:11::1/128 via 16::1, multicast distance 1 Route resolves outside the table
  ```

Workaround: There is no workaround.

- CSCua35161

  Symptom: On the DMVPN HUB, some crypto maps still exist after removing Tunnel protection from the Tunnel interface.

  Conditions: This symptom occurs with scaling test.

  Workaround: There is no workaround.

- CSCua55797

  Symptoms: The **privilege exec level 0 show glbp brief** command causes the memory to be depleted when the **show running** or **copy running-config startup-config** commands are used. The configurations will then show this:

  ```
  privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief brief brief
  brief brief privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief
  brief brief brief privilege exec level 0 show glbp GigabitEthernet0/0 brief brief
  brief brief brief privilege exec level 0 show glbp GigabitEthernet0/0 brief brief
  brief brief privilege exec level 0 show glbp GigabitEthernet0/0 brief brief brief
  privilege exec level 0 show glbp GigabitEthernet0/0 brief brief privilege exec level 0
  show glbp GigabitEthernet0/0 brief privilege exec level 0 show glbp privilege exec
  level 0 show
  ```

  Removing the configurations causes this to happen over and over until the telnet session is terminated:

  ```
  priv_push : no memory available priv_push : no memory available priv_push : no memory
  available priv_push : no memory available priv_push : no memory available
  ```

  If the configurations are saved and device is reloaded, the device will not fully boot until the configurations are bypassed.

  Conditions: This issue happens after the **privilege exec level 0 show glbp brief** command is entered and saved.

  Workaround: Reload the router before saving the configurations.

- CSCua75781

  Symptoms: CME reloads for E911 call ELIN translation for incoming FXS/FXO trunk.

  Conditions: The symptom is observed from Cisco IOS interim Release 15.3(0.2)T.

  Workaround: There is no workaround.

- CSCub04965

  Symptom: Multiple symptoms may occur including:

  - Multiple sessions established to TACACS+ server which never clear are seen in the output of **show tcp brief**.
  - Pings to the loopback address from directly connected equipment suffers packet loss.
  - Traffic and pings through the switch suffers packet loss.
  - CPU utilization remained stable and below 10% when the issue was occurring, the interface counters were not reporting any errors or drops.
  - TACACS+ authentication errors, authorization errors, or accounting errors.
  - SSH/TELNET via VTY not accessible.
  - If condition exists for a period of time the switch may stop passing traffic.

Conditions: The symptom is observed when the device is configured with TACACS+. It is seen mostly on Cisco 3750/3760 switches, but has been observed on Cisco 6500 switches.

Workaround:

- Remove the AAA and TACACS+ server configuration.
- Clear the existing TCP connections with **clear tcp tcb**.
- Reconfigure the TACACS+ server configuration to use “single-connection” mode.
- Reconfigure the AAA configuration.

Mitigation using EEM: A Cisco IOS Embedded Event Manager (EEM) policy that is based on Tool Command Language (Tcl) can be used on vulnerable Cisco IOS devices to identify and detect a hung, extended, or indefinite TCP connection that causes the symptoms to be observed. The policy allows administrators to monitor TCP connections on a Cisco IOS device. When Cisco IOS EEM detects hung or stale TCP connections, the policy can trigger a response by sending a syslog message or a Simple Network Management Protocol (SNMP) trap to clear the TCP connection. The example policy provided in this document is based on a Tcl script that monitors and parses the output from two commands at defined intervals, produces a syslog message when the monitor threshold reaches its configured value, and can reset the TCP connection. The EEM script is available at:

https://supportforums.cisco.com/docs/DOC-19344

- CSCub18622

  Symptom: Dynamic ACL does not get applied to the interface ACL, but the user shows up in the **show ip auth-proxy cache** command output.

  Conditions: This symptom occurs when auth proxy is configured on a tunnel interface.

  Workaround: Move the auth-proxy rules onto a physical interface.

- CSCub34534

  Symptom: A basic call between 2 SIP phones over SIP trunk (KPML-enabled) fails.

  Conditions: This symptom is observed with Cisco ISR G2 platforms.

  Workaround: There is no workaround.

- CSCub40547

  Symptoms: ES+ module crashes with the followoing error message:

  ```
  %NP_DEV-DFC1-2-WATCHDOG: Watchdog detected on NP 0
  ```

  Conditions: The issue is specific to the type of packet and its content which is unique when vidmon is configured.

  Workaround: Remove vidmon configuration.

- CSCub46423

  Symptoms: Connecting from Windows 7 L2TP/IPSec client to the VPN fails when using HSRP virtual IP as a gateway IP and Error 788 is displayed.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T or later releases, and the Windows 7 L2TP/IPsec VPN client.

  Workaround: Downgrade to Cisco IOS Release 15.1(3)T.

- CSCub52278

  Symptom: The DVTI Virtual Access interface may flap during rekey with a large number of IKEv2/IPSec tunnels.

Conditions: This symptom occurs when IKEv2 is used in large scale deployment.

Workaround: There is no workaround.

- CSCub68199

  Symptom: A Cisco Router configured for IPv6/IPv4 Native IP Routes or l2-connected ISG sessions may reload with following errors in crashinfo:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = IP Inband Session Initiator
  ```

  Conditions: This symptom occurs due to high or extended duration of setup and tear-down rate of sessions. Time to potential reload can vary depending on call volume and duration of session cycling.

  Workaround: There is no workaround.

- CSCub93641

  Symptom: The load balancing feature of the Flex-VPN solution of Cisco IOS does not provide authentication facilities to avoid a non authorized member to join the load balancing cluster. Thus, an attacker may impact the integrity of the Flex-VPN system by inserting a rogue cluster member and having the load balance master to forward a VPN session to it. A number of secondary effects, including black-holing of some of the VPN traffic may be triggered by this issue.

  Conditions: This symptom occurs in Flex-VPN with the Load Balancing feature active.

  Workaround: Using CoPP and interface access-list may be used to allow only trusted router to join the load balancer cluster

  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 4.3/3.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:N/E:F/RL:W/RC:C

  CVE ID CVE-2012-5032 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

- CSCub95285

  Symptoms: No logging messages are seen when configuring the syslog server in CLI mode until configuration mode is exited. However when unconfiguring the syslog server, syslog messages will appear within configuration mode.

  Conditions: The symptom is observed when, in CLI configuration mode, you enter the following command:

  ```
  Router(config)#logging host 1.2.3.4 transport tcp
  ```

  Workaround: There is no workaround.

- CSCuc08477

  Symptom: All EOS and non EOS entries are missing for mLDP labels in the mid/bud node.

  Conditions: This symptom may occur due to random path flap mLDP tree changes.

  Workaround: Removing and adding the mLPD tree will trigger re-programming.

- CSCuc11958

  Symptom: 7600-SIP-400 linecard crash seen with SPA reload.

  Conditions: The symptom is observed with a SPA reload.

  Workaround: There is no workaround.

- CSCuc22651

  Symptom: A router may experience a crash in the “BGP Task” process during best path selection.

  Conditions: In a rare corner case, when the last remaining paths are deleted around the same time by two different threads of execution, a null pointer exception can be raised in the “BGP Task” process.

  Workaround: There is no workaround.

- CSCuc25995

  Symptoms: A router unexpectedly reboots and a crashinfo file is generated. The crashinfo file contains an error similar to the following:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 04:52:23 UTC Wed Sep 19 2012 addr=0x4,
  pc=0x26309630z , ra=0x26309614z , sp=0x3121BC58
  ```

  Conditions: This occurs when IPsec is used. More precise conditions are not known at this time.

  Workaround: There is no workaround.

- CSCuc34973

  Symptom: There is a CPU hog with G8302.

  Conditions: This symptom occurs when the router is reloaded.

  Workaround: There is no workaround.

- CSCuc47356

  Symptoms: Static routes are not getting removed.

  Conditions: This symptom is observed with Smap - Smap. Removal of CLI does not remove the static route.

  Workaround: Remove the ACL before removing the SA.

- CSCuc51879

  Symptom: Traffic loss occurs on the Cisco ASR 1000 Series Routers during an RP SSO switchover.

  Conditions: This symptom occurs during an RP SSO switchover on the Cisco ASR 1000 Series Routers.

  Workaround: There is no workaround.

- CSCuc59858

  Symptoms: Valid dynamic authorization requests which are not retransmissions are marked as retransmission.

  Conditions: This may occur when valid dynamic authorization requests with the same RADIUS packet identifier is sent from different source ports.

  Workaround: There is no workaround.

- CSCuc61302

  Symptoms: The symptoms for XE38, XE37 and mcp_dev are different for this DDTS. On mcp_dev, VPLS PW is not coming up, but on XE37 and XE38, static mac commands are missing after a reload.

  Conditions: This occurs only on reload. The configured static mac commands are missing after a reload.

  Workaround: There is no workaround other than re-entering the static mac commands.

- CSCud02391

  Symptoms: The EIGRP routes are not coming up after removing and reenabling the tunnel interface.

  Conditions: This symptom is observed when EIGRP routes do not populate properly.

  Workaround: There is no workaround.

- CSCud11078

  Symptoms: Removal of the service instance on the target device causes a crash.

  Conditions: This symptom is not consistently reproducible on all configurations as the underlying cause is a race condition.

  Workaround: De-schedule the probe before removing the service instance.

- CSCud13768

  Symptom: RP crashes while trying to verify UDP-JITTER in IP SLAs VRF-lite.

  Conditions: This symptom occurs while trying to verify IP SLAs UDP Jitter operation.

  Workaround: There is no workaround.

- CSCud24806

  Symptom: Compared to V1 ATM SPA, V2 SPAs have more latency and bad bandwidth partition.

  Conditions: The symptom is observed under the following conditions:

  1. V2 SPA configured in L3 QoS mode.
  2. Policy map contains “no priority queue”.
  3. Policy map has more than one QoS class.
  4. Each class has a WRED profile configured.

  Workaround: While using a policy-map with a WRED profile, use the drop-probability value as 8. This improves the partition.

- CSCud45339

  Symptom: The **ping mpls tp tunnel-tp lsp act** indicates that the LSP is unreachable even though it is functioning correctly.

  Conditions: This symptom occurs during MPLS Transport Profile (TP) and OAM GAL handling.

  Workaround: There is no workaround.

  More Info: The MPLS Generic Associated Channel (GAL) may not be processed in the exception handling path, which impacts OAM ping mpls for tunnel-tp.

- CSCud55286

  Symptoms: Traffic drops for sometime after doing a switchover.

  Conditions: The symptom is observed when a switchover is performed on a Cisco ASR 903.

  Workaround: Put a neighbor command where the neighbor has no meaning and will never be up. This will solve the timing issue.

- CSCud58457

  Symptom: Standby interface stays UP/UP after a reload:

  ```
  BGL.S.15-ASR1004-1#sh int des Interface Status Protocol Description Te0/0/0 down down
  Te0/1/0 up up Te0/2/0 down down Te0/3/0 up up Gi0 admin down down
  ```

  It should be like this :

```
BGL.S.15-ASR1004-1#sh int des Interface Status Protocol Description Te0/0/0 down down
Te0/1/0 up up Te0/2/0 down down Te0/3/0 standby mode down Gi0 admin down down
```

Conditions: The symptom is observed when “backup interface” and “carrier-delay” are configured under the interface:

```
interface TenGigabitEthernet0/1/0 backup interface TenGigabitEthernet0/3/0 ip address
10.163.137.29 255.255.255.224 logging event link-status carrier-delay up 1
carrier-delay down msec 0 cdp enable hold-queue 4096 in hold-queue 4096 out !
interface TenGigabitEthernet0/3/0 mac-address d867.d9dd.ff10 no ip address logging
event link-status carrier-delay up 1 carrier-delay down msec 0 cdp enable hold-queue
4096 in hold-queue 4096 out !
```

Workaround: Flap the standby interface.

- CSCud83835

  Symptoms: An IPsec VPN tunnel fails to be established. The **debug crypto ipsec** command shows no output when attempting to bring up the tunnel.

  Conditions: This symptom occurs when all of the following conditions are met:

  1. The crypto map is configured on a Virtual-Template interface.
  2. This Virtual-Template interface is configured with “ip address negotiated”.
  3. The tunnel is initiated locally (in other words, if the tunnel is initiated by the peer, it comes up correctly).

  Workaround: Downgrade to Cisco IOS Release 15.2(2)T3 or earlier releases or always initiate the VPN tunnel from the peer.

- CSCud86954

  Symptom: Some flows are not added to the Flexible Netflow cache, as indicated by the “Flows not added” counter increasing in the **show flow monitor statistics** command output. “Debug flow monitor packets” shows “FNF_BUILD: Lost cache entry” messages, and after some time, all cache entries are lost. At that moment, debug starts showing “FLOW MON: ip input feature builder failed on interface couldn’t get free cache entry”, and no new entries are created and exported (“Current entries” counter remains at 0).

  The following is sample output when all cache entries are lost:

  ```
  Router#sh flow monitor FNF-MON stat Cache type: Normal Cache size: 4096 Current
  entries: 0 High Watermark: 882
  Flows added: 15969 Flows not added: 32668 Flows aged: 15969 - Active timeout ( 1800
  secs) 0 - Inactive timeout ( 15 secs) 15969 - Event aged 0 - Watermark aged 0 -
  Emergency aged 0
  ```

  Conditions: This symptom occurs when all of the following are true:

  – Flexible Netflow is enabled on a DMVPN tunnel interface.
  – Local policy-based routing is also enabled on the router.
  – Local PBR references an ACL that does not exist or an ACL that matches IPsec packets.

  Workaround:

  1. Make sure that the ACL used in the local PBR route-map exists and does not match IPsec packets sent over the DMVPN tunnel interface.
  2. Disabling encryption on the tunnel interface, or changing tunnel mode from mGRE to GRE also removes this bug.
  3. The issue will not be seen if FNF is not configured, or if FNF is configured but is not monitoring VPN traffic.

- CSCud88483

  Symptom: In a GETVPN and IPsec redundant configuration combination, if you reload a secondary group member in the topology it will cause TEK registration of the group member to be lost once the router comes back up and the HSRP does a state transition to standby.

  Conditions: The symptom is observed with a GETVPN with IPsec redundancy configuration.

  Workaround: Wait for the next rekey or issue **clear crypto gdoi**.

- CSCue01146

  Symptom: SNMP GET fails for VPDN-related MIB.

  Conditions: This symptom occurs while receiving an SNMP GET for the MIB before all VPDN configurations are applied.

  Workaround: Reload the router.

- CSCue09385

  Symptom: Active RP crash during sessions bring up after clearing PDP.

  Conditions: The symptom is observed after clearing PDP.

  Workaround: There is no workaround.

  More Info: This is a negative test where DHCP IP under APN on IWAG is the access interface IP. In real world, we do not configure access interface IP as a DHCP IP for an APN.

- CSCue25526

  Symptom: Router crashes when configuring FNF interface bind.

  Conditions: This symptom occurs when an interface bind is removed in a session before the first session bind is complete.

  Workaround: Do not remove the bind in the second session until the first session bind is complete.

- CSCue28318

  Symptoms: A Cisco router doing authentication proxy may unexpectedly reload when running the **test aaa command** command.

  Conditions: This symptom occurs when the router is using LDAP authentication and has a misconfigured LDAP authentication configuration.

  Workaround: Correct the misconfiguration.

- CSCue32707

  Symptom: crypto pki export <> causes crash.

  Conditions: This symptom is observed in when a SUB CA trustpoint is configured and a trustpoint is configured and enrolled to that SUB CA.

  Workaround: If possible, have the trustpoint on a separate box.

- CSCue39518

  Symptom: A Cisco 7200 with VSA fails to encrypt traffic under specific conditions.

  Conditions: The symptom is observed under the following conditions:

  - Cisco 7200 has IPsec SSO configured with HSRP. Dynamic crypto map is configured. Remote sides have static crypto map to this device.
  - All the 15.x codes to the latest Cisco IOS 15.2(4)M2 are affected.
  - Issue is not seen in the Cisco IOS 12.4 codes.

  - Issue not seen when IPsec SSO and HSRP are removed.

  Workaround: There is no workaround.

- CSCue47586

  Symptom: For an MGRE tunnel, internal VLANs are not allocated in the standby supervisor.

  Conditions: The symptom is observed when an HA router boots up with MGRE tunnel configurations. Internal VLANs are not allocated in the standby supervisor due to a sync issue during bootup.

  Workaround: There is no workaround.

- CSCue57495

  Symptom: Traceback is observed with the following error message:

  ```
  standby cannot allocate VLAN for Tunnel Rsvd Vlan
  ```

  Conditions: The issue seen while configuring L2VPN and L3VPN with scaled tunnel configurations.

  Workaround: There is no workaround.

- CSCue59592

  Symptom: Multiple crashes observed with the following tracebacks after upgrading the Cisco IOS Release from 12.2(33)SRC1 to 12.2(33)SRE6:

  ```
  *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to lock a
  semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
  9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
  9E19F1C 9E1D4FC *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to
  lock a semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
  9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
  9E19F1C 9E1D4FC *Jul 27 01:39:33 SUM: %SCHED-3-SEMLOCKED: CMFI RP process attempted to
  lock a semaphore, already locked by itself -Traceback= 87807BC 999A314 9E1684C 9E17E4C
  9E18074 AA9B25C AA9B2C8 AAAA270 A1D33B4 A1D3474 A1D61A4 A1D14B0 AAC8A28 9E1909C
  9E19F1C 9E1D4FC
  ```

  Conditions: The symptom is observed with a combination of BGP VPNv4 prefixes + PBR enabled on the interface for the VRF and during upgrade of image or reload of the device. If “mls mpls recirc agg” is enabled in global mode, then this crash will not be observed.

  Workaround: Enable “mls mpls recirc agg” in global mode.

- CSCue65405

  Symptom: SAs do not get installed in GETVPN GM.

  Conditions: The symptom is observed when the key server is configured with “receive-only” SAs.

  Workaround: Remove receive-only configuration at the key server.

- CSCue65498

  Symptoms: Wrong CIR is getting cloned to the VA interface.

  ```
  Dialer1 Service-policy output: OPT3-DIALER-4b-TR25 Class-map: CRI-OUT (match-any)
  police: cir 8 % cir 819000 bps, bc 25593 bytes <<<<<
  Virtual-Access3 Service-policy output: OPT3-DIALER-4b-TR25 Class-map: CRI-OUT
  (match-any) police: cir 8 % cir 8000000 bps, bc 250000 bytes <<<<<
  ```

  Conditions: This symptom is observed with the PPPoE dialer/client configuration.

  Workaround: Remove and reapply the service-policy under the Dialer interface.

- CSCue68761

  Symptom: A leak in small buffer is seen at ip_mforward in Cisco IOS Release 15.1(4)M3.

```
Device: Cisco 2911 Cisco IOS: c2900-universalk9-mz .SPA.151-4.M3.bin
------------------ show buffers ------------------
Buffer elements: 156 in free list (500 max allowed) 11839912 hits, 0 misses, 617
created
Public buffer pools: Small buffers, 104 bytes (total 45187, permanent 50, peak 45187 @
10:04:00): 0 in free list (20 min, 150 max allowed) 7968057 hits, 202704 misses, 2128
trims, 47265 created 71869 failures (680277 no memory)
------------------ show buffers usage ------------------
Statistics for the Small pool Input IDB : Mu1 count: 45180 Caller pc : 0x22CF95C4
count: 45180 Resource User: IP Input count: 45180 Caller pc : 0x22381654 count: 2
Resource User: Init count: 2 Output IDB : Mu1 count: 4 Caller pc : 0x2380114C count: 4
Resource User: PIM regist count: 4 Number of Buffers used by packets generated by
system: 45187 Number of Buffers used by incoming packets:
++++++++++++++++++++++++++++small buffer packet++++++++++++++++++++++++++++++++
<snip>
Buffer information for Small buffer at 0x2A815220 data_area 0xD9DEB04, refcount 1,
next 0x0, flags 0x2080 linktype 7 (IP), enctype 16 (PPP), encsize 2, rxtype 1 if_input
0x30F21520 (Multilink1), if_output 0x0 (None) inputtime 00:02:46.212 (elapsed
05:55:11.464) outputtime 00:01:22.632 (elapsed 05:56:35.044), oqnumber 65535
datagramstart 0xD9DEB56, datagramsize 38, maximum size 260 mac_start 0xD9DEB56,
addr_start 0x0, info_start 0xD9DEB58 network_start 0xD9DEB58, transport_start
0xD9DEB6C, caller_pc 0x22CF0044
source: 10.131.124.33, destination: 224.0.1.40, id: 0x55F0, ttl: 11, TOS: 192 prot:
17, source port 496, destination port 496
Enter hex value: 0x22CF95C4 0x22CF95C4:ip_mforward(0x22ce9448)+0x51c Enter hex value:
0x22CF0044 0x22CF0044:ip_mforward(0x22ce9448)+0x51c
```

  Conditions: This symptom is observed with the Cisco 2911 running Cisco IOS Release 15.1(4)M3. When IP Multicast is used with NAT, in certain scenarios when NAT functionality returns error, multicast code does not free duplicate packet buffers eventually leading to exhaustion of packet buffer pool in the router.

  Workaround: There is no real workaround except to disable NAT.

- CSCue74612

  Symptom: FTP download fails in FTS client.

  Conditions: The symptom is observed with FTS transfer over FTP via VRF.

  Workaround: There is no workaround.

- CSCue75986

  Symptom: The active route processor crashes because of a segmentation fault in the PIM IPv6 process after de-configuring a VRF.

  Conditions: This symptom is observed when BGP, multicast-routing, or a VRF is de-configured while VRF-forwarding for the affected VRF is still configured on some interfaces and IPv6 multicast state entries exist within the affected VRF.

  Workaround: Before removing a VRF using **no vrf definition xxx**, de-configuring “router bgp ...” or de-configuring multicast-routing for any VRF or for the global routing table, de-configure the IPv6 and the IPv4 MDT tunnels for affected VRFs as follows:

  1. Under the “vrf definition ...”/ “address-family ipv6” configuration sub-mode, execute **no mdt default ...**.
  2. Under the “vrf definition ...”/ “address-family ipv4” configuration sub-mode, execute **no mdt default ...**.

- CSCue76057

  Symptom: On a SIP 400 with gigeV2 SPA, when EVC is configured with “encap default”, it is seen that sometimes the FUGU TCAM is not programmed with correct VVID for the EVC. This results in incoming traffic reaching the linecard with wrong VVID. This can impact traffic incoming on the EVC.

  Conditions: The symptom is observed with an “encap default” configuration under EVC, or removal and re-application of “encap default” under EVC.

  Workaround: There is no workaround.

- CSCue76102

  Symptoms: Redistributed internal IPv6 routes from v6 IGP into BGP are not learned by the BGP neighboring routers.

  Conditions: This symptom occurs because of a software issue, due to which the internal IPv6 redistributed routes from IGPs into BGP are not advertised correctly to the neighboring routers, resulting in the neighbors dropping these IPv6 BGP updates in inbound update processing. The result is that the peering routers do not have any such IPv6 routes in BGP tables from their neighbors.

  Workaround: There is no workaround.

- CSCue81327

  Symptoms: Standby RP crashes during bulk sync with:

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

  Conditions: The crash occurs while syncing a shutdown TE tunnel interface configuration.

  Workaround: Delete the shutdown TE tunnel configuration, if not required.

- CSCue89779

  Symptom: A FlexVPN spoke configured with an inside VRF and front-door VRF may have problems with spoke-to-spoke tunnels if they are not the same. During tunnel negotiation, two Virtual-access interfaces are created (while only one is needed), the one in excess may fail to cleanup correctly. As a result, the routes created by NHRP process may lead to loss of traffic, or traffic may continue to flow through the Hub.

  Conditions: This symptom occurs when the VRF used on the overlay (IVRF) and the VRF used on the transport (FVRF) are not the same.

  Workaround: There is no workaround.

- CSCue94653

  Symptom: When the port-security configured interface goes to blocking state (MST), the VLANs configured on the port go to not-forwarding state temporarily. The secure mac-addresses are not added back resulting in loss of traffic.

  Conditions: The symptom is observed when the port-security configured interface goes to blocking state.

  Workaround: Shut and no shut the port-security interface to re-add the mac-addresses.

- CSCuf03079

  Symptom: A Cisco IOS router running with ISIS remote-LFA configured can crash.

  Conditions: This symptom occurs when shut/no shut is performed on an interface multiple times.

  Workaround: Disable the ISIS remote-LFA configuration.

- CSCuf09006

  Symptoms: Upon doing a **clear ip bgp * soft out** or **graceful shutdown** on a PE, all VPNv4/v6 routes on an RR from this PE are purged at the expiry of enhanced refresh stale-path timer.

  Conditions: The symptom is observed with the following conditions:

  1. 1. PE must have BGP peering with at least one CE (VRF neighbor) and at least one RR (VPN neighbor).
  2. PE must have a rtfilter unicast BGP peering with the RR.
  3. IOS version must have “Enhanced Refresh” feature enabled.
  4. A **clear ip bgp * soft out** or **graceful shutdown** is executed on the PE.

  Workaround: Instead of doing **clear ip bgp * soft out**, do a route refresh individually towards all neighbors.

- CSCuf09198

  Symptom: After deleting a VRF, you are unable to reconfigure the VRF.

  Conditions: The symptom is observed when BGP SAFI 129 address-family is not configured, but unicast routes are installed into multicast RIB to serve as upstream multicast hop, as described in RFC 6513. This applies to VRFs configured before BGP is configured.

  Workaround: Beyond unconfiguring BGP, there is no workaround once the issue occurs. Configuring a dummy VRF multicast address-family under BGP before the issue occurs can prevent the problem from occurring.

- CSCuf30798

  Symptom: SIP 600 crashes.

  Conditions: The symptom is observed with VPLS VC going over GRE tunnel and chassis having both ES+ and SIP 600 card.

  Workaround: Remove VPLS over GRE. This configuration is not supported.

- CSCuf56776

  Symptom: After a linecard is removed and reinserted (OIR), traffic may fail to pass through some virtual circuits which have been configured for pseudowire redundancy.

  Conditions: This symptom is observed when the first segment ID in the redundancy group is numerically greater than the second segment.

  ```
  PE1#show ssm id | inc 1st 1stMem: 16394 2ndMem: 12301 ActMem: 12301 1stMem: 16394
  2ndMem: 12301 ActMem: 12301
  ```

  After the OIR is performed, it can be seen that the segments are reversed on the linecard.

  ```
  ESM-20G-12#sh ssm id | inc 1st 1stMem: 12301 2ndMem: 16394 ActMem: 12301 1stMem: 12301
  2ndMem: 16394 ActMem: 12301
  ```

  Workaround: There is no workaround.

- CSCuf60830

  Symptom: Standby-RP occasionally crashes on process SSS Manager after an RP failover when the new Standby-RP attempts to sync.

  Conditions: This symptom occurs during an RP Failover, at high scale, with a high churn of sessions and ISG services.

  Workaround: There is no workaround.

- CSCuf61640

  Symptom: Tracebacks as follows seen during router bootup:

  ```
  %SYS-2-INTSCHED: 'suspend' at level 2 -Process= "Init", ipl= 2, pid= 3
  -Traceback= 4F6966C 6A708EC 890127C 6B4F924 6B4F7F8 6B4EAAC 6B4F43C 6B4F514 6DD6D4C
  6DDB3A8 6A23E50 6A23F18 6A24100 57D3F94 57D42D8 4F701E4
  0x4F6966C ---> process_ok_to_reschedule+288 0x6A708EC ---> process_suspend+4C
  0x890127C ---> random_fill+248 0x6B4F924 ---> default_entropy_routine+9C 0x6B4F7F8
  ---> hardware_entropy_source+CC 0x6B4EAAC ---> nist_instantiate+78 0x6B4F43C --->
  try_create_rng+1B4 0x6B4F514 ---> nist_rng+34 0x6DD6D4C --->
  cts_sap_get_key_counter+54 0x6DDB3A8 ---> cts_sap_init+C4 0x6A23E50 --->
  subsys_init_routine+60 0x6A23F18 ---> subsys_init_class_internal+A8 0x6A24100 --->
  subsys_init_class+8C 0x57D3F94 ---> system_init+250 0x57D42D8 ---> init_process+94
  0x4F701E4 ---> ppc_process_dispatch+
  ```

  Conditions: The symptom is observed during router bootup.

  Workaround: There is no workaround.

- CSCuf62756

  Symptom: If **bandwidth qos-reference** *value* is configured on an interface which bandwidth can change, then the actual interface bandwidth will be used for QoS service-policy validation when the interface bandwidth changes. This can result in a service-policy being removed if the interface bandwidth is insufficient to meet the requirements of the service-policy, such as bandwidth guarantees.

  Conditions: This symptom occurs in variable-bandwidth interfaces such as EFM interfaces or PPP multilink bundles.

  Workaround:

  1. Use proportional actions in the QoS service-policy, such as "police rate percent....", "bandwidth remaining ratio...", "bandwidth remaining percent...", and "priority percent"
  2. You can configure **bandwidth qos-reference** with maximum bandwidth of the interface:

  interface Ethernet0 bandwidth qos-reference <*max bandwidth of interface*>

  This can prevent policy-map detached due to interface bandwidth change.

- CSCuf64313

  Symptoms: Linecard crash is seen with machine-check exception.

  Conditions: There is no trigger. The crash is random.

  Workaround: There is no workaround.

- CSCuf65371

  Symptom: On LAC, with "l2tp hidden" configured under VPDN template, L2TP sessions are failing to establish on existing L2TP tunnels after RP failover.

  Conditions: The symptom is observed with "l2tp hidden" configured under VPDN template.

  Workaround: Tear down L2TP tunnels after RP failover, or unconfigure "l2tp hidden". Disabling L2TP redundancy with "no l2tp sso enable" will fix issue as well.

- CSCuf68995

  Symptom: Ping failures. Traffic gets dropped.

  Conditions: The symptom is observed when you configure MPLSoMGRE tunnel on PE1 and PE2. Initiate ping from CE1 to CE2. Packets reach the CE2 and replay is coming back but these packets are getting dropped on PE2. After PE2 switchover, ping fails from CE1 to CE2. PE2 is configured with MPLSoMGRE on an HA system. Topology:

```
CE1---- PE1 ----PE2----CE2
```

Workaround: There is no workaround.

- CSCuf81275

  Symptom: Some ISG sessions do not pass traffic.

  Conditions: This symptom is observed when you have more than one Line Card for the ISG sessions.

  Workaround: There is no workaround.

- CSCuf82179

  Symptom: BGP routes remain installed in multicast RIB even after “address-family” configuration has been removed from “vrf definition”.

  Conditions: This symptom is observed in MVPN topology, where the stale routes are installed as an upstream multicast hop, as described in RFC: http://tools.ietf.org/html/rfc6513

  Workaround: There is no workaround.

- CSCuf93376

  Symptom: CUBE reloads while testing SDP passthrough with v6.

  Conditions: The symptom is observed while testing SDP passthrough with v6.

  Workaround: There is no workaround.

- CSCuf93606

  Symptoms: A Cisco 3945E router crashes.

  Conditions: The symptom is observed with the following conditions:

  – Extension mobility is configured for the phone. The logout profile should not be configured with any number.
  – In the logged out state, user has to press the “NewCall” softkey followed by dialing any digit between 1-9 (excluding 0).
  – Instead of pressing “dial” softkey, press “AbbrDial” softkey.

  Workaround: Have a proper number configured under the logout profile.

- CSCug04187

  Symptom: Build breakage.

  Conditions: This symptom occurs due to CSCuf62756.

  Workaround: There is no workaround.

- CSCug08561

  Symptom: After a web-logon, users do not get the web-logon response page sent by the portal. If the web-logon is successful, users are not redirected to the web address which they have entered initially but are redirected to the portal for authentication.

  Conditions: This symptom occurs under the following conditions:

  1. Walkby feature is enabled with L4R & PBHK features applied to the lite session.
  2. User initiated the web-logon request.

  Workaround: There is no workaround.

  More Info: When a user does a web-logon, an account-logon coa request is triggered from the portal to ISG. In ISG, the account-logon request triggers a lite session conversion to a dedicated session. During the conversion, lite session and its associated resources (L4R and PBHK mappings) are

removed from PD and a dedicated session gets provisioned. Once the conversion is done, ISG replies back with COA ACK/NACK to the portal. Based on the response from ISG, the portal generates a weblogon response (SUCCESS/FAILURE) page and sends it back to the client. But when it reaches ISG, the response packet does not get classified to session in the downstream direction and gets dropped in ISG because PBHK & L4R maping are deleted.

- CSCug10922

  Symptom: A traceback is seen in the standby RP after a headend SSO.

  Conditions: This symptom occurs when SSO tracebacks are seen.

  Workaround: There is no workaround.

- CSCug15952

  Symptom: %QOS-3-INDEX_EXISTS error message is shown and router crashes.

  Conditions: The symptom is observed when sessions are bought up and the collision IDs with dynamic policy names are synced to standby from active. When the sessions time out and restart, the same dynamic policy names are synced to HA tree on standby again without cleaning up the tree earlier and the crash will happen.

  Workaround: Avoid the same session reestablishment before rebooting the router.

- CSCug17724

  Symptom: When using session protection and graceful restart for LDP, LDP neighbor goes down immediately after filtering LDP hello between routers. The LDP neighbor should go down after 10 minutes (default value of forwarding state holding time for GR).

  Conditions: The symptom is observed when you enable session protection and graceful restart for LDP

  Workaround: There is no workaround.

- CSCug17808

  Symptom: Redistributed default route not advertised to EIGRP peer.

  Conditions: This symptom is observed when Cisco ASR router is rebooted or the route is cleared via the **clear ip route** command, the route disappears form the spokes.

  Workaround: Clearing the EIGRP Neighborship restores the route on the spokes.

- CSCug18797

  Symptom: Router crashes when it checks whether the interface is configured as DHCP SIP session initiator.

  Conditions: The symptom is observed DHCP and ISG are configured.

  Workaround: There is no workaround.

- CSCug20048

  Symptom: MPLS traffic engineering BC MAM model does not take effect when configured.

  Conditions: The symptom is observed when you configure the BC MAM model.

  Workaround: There is no workaround.

- CSCug20705

  Symptom: A 7600-SIP-400 LC crash is seen with an SPA reload.

  Conditions: This symptom occurs after an SPA reload with FRF12 and service policy on the interface.

Workaround: There is no workaround.

- CSCug23348

  Symptom: The “mod” value in the SSRAM may be inconsistent to the number of ECMP paths.

  Conditions: This occurs with ECMP TE tunnels with **tunnel mpls traffic-eng load-share** *value* commands configured.

  Workaround: Remove the **tunnel mpls traffic-eng load-share** *value* commands from the TE tunnels.

- CSCug24114

  Symptom: CTS environment-data download fails from ISE.

  Conditions: The symptom is observed if there is less PAC and environment-data refresh timer is configured in ISE. After multiple refreshes of PAC and environment data and the switch is reloaded, sometimes a CTS environment-data download fails from ISE on the switch.

  Workaround: Unconfigure **pac key CLI** and configure it again as below:

  ```
  no pac key pac key <key-id>
  ```

- CSCug25258

  Symptom: Router crashes while running the **show interface rate-limit** command. When entries down the list of the output disappear for reasons such as interfaces going down or PPPoE clients disconnecting, the router may crash when you hit the space bar to get to these invalid entries.

  Conditions: This symptom occurs when rate limiting is configured.

  Workaround: Configure **term length 0** before running the show output.

- CSCug28904

  Symptoms: Router drops ESP packets with CRYPTO-4-RECVD_PKT_MAC_ERR.

  Conditions: The symptom is observed when the peer router sends nonce with length 256 bytes.

  Workaround: There is no workaround.

- CSCug31561

  A vulnerability in the DHCP implementation of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  The vulnerability occurs during the parsing of crafted DHCP packets. An attacker could exploit this vulnerability by sending crafted DHCP packets to an affected device that has the DHCP server or DHCP relay feature enabled. An exploit could allow the attacker to cause a reload of an affected device.

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

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-dhcp

  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight 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 September 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_sep13.html

- CSCug33084

  Symptom: SP/DFC crash is seen when churn on multicast is done, either through provisioning/unprovisioning or other network event.

  Conditions: The issue occurs when a pointer to an already freed hal_context is still present in a replicate queue. Later during churn the same pointer is accessed which leads to the crash.

  Workaround: There is no workaround.

- CSCug34404

  Symptom: RP crash seen at be_interface_action_remove_old_sadb.

  Conditions: The symptom is observed while unconfiguring the 4K SVTI sessions after an HA test.

  Workaround: There is no workaround.

- CSCug34503

  Symptom: LLDP packets with destination MAC: 01:80:C2:00:00:0E are dropped.

  Conditions: This symptom occurs with the fix of CSCue41216.

  Workaround: There is no workaround.

  More Info: Regression because of CSCue41216 causes LLDP packets which have a MAC address of 01.80.c2.00.00.0e to get dropped according to MEF standard. But the packets should get dropped for SUNI and NNI port, while for CUNI they should get passed.

- CSCug34507

  Symptom: Traffic decrypted on a Cisco ISR G2 series is process switched instead of staying in the CEF path.

  Conditions: The symptom is observed when the hub and/or the spoke are located behind NAT or PAT.

  Workaround: Disable NAT/PAT.

- CSCug34877

  Symptom: A switch crashes with following message:

  ```
  %SYS-2-LINKED: Bad enqueue of 901E0D40 in queue 1AABE690 -Process= "SSH Process", ipl= 0, pid= 392
  ```

  Conditions: This symptom occurs while making an SSH connection to a remote device from the switch while having multiple SSH connections to the same switch

  Workaround: There is no workaround.

- CSCug37242

  Symptoms: Router crash due to memory leak.

  Conditions: The symptom is observed with a CME shared line feature configuration.

  Workaround: Disabling shared line feature will avoid memory leak.

- CSCug38011

  Symptom: Device crashes with CPU hog messages.

  Conditions: The symptom is observed when the device is reloaded after configuring NTP peer:

  ntp server pool.ntp.org source cell0

  Workaround: There is no workaround.

- CSCug39278

  Symptom: L3 QoS policy not working in EVC L3 VPN.

  Conditions: The symptom is observed when CFM is enabled globally.

  Workaround: Disable CFM.

- CSCug44667

  Symptom: SG3 fax call failures observed for STCAPP audio calls.

  Conditions: Fax CM tone detection is turned ON even when all fax and modem related configurations have been disabled on the STCAPP gateway.

  Workaround: STCAPP modem pass-through feature can be enabled, but you may run into issues with some answering SG3 fax machines which have stringent requirements for fax CM signal.

- CSCug50208

  Symptom: A crash is seen due to double free of memory.

  Conditions: The symptom is seen when the accept interface VLAN goes down.

  Workaround: There is no workaround.

- CSCug50340

  Symptom: PW traffic is not flowing after SSO/card reset the active PTF card.

  Conditions: The symptom is observed with the following conditions:

  1. Create a unprotected tunnel between the active PTF card and create a PW.
  2. Apply the table map. Bi-directional traffic is flowing fine.
  3. SSO/reset the active PTF card in node 106 (4/1).
  4. Now tunnel core port is in standby card.
  5. Observed bi-directional traffic is not flowing once the card becomes up.
  6. Again reset the active PTF card (5/4).
  7. Observe uni-directional traffic only is flowing.

  Workaround: Delete the PW and recreate it again. However, note that if you do an SSO/card reset, the issue reappears.

- CSCug52119

  Symptom: A RIB route is present for a prefix, but the router continues to LISP encapsulate.

  Conditions: The symptom is observed when a LISP map-cache existed for a prefix and then the RIB route was added later.

  Workaround: Use the following command:

  ```
  clear ip/ipv6 lisp map-cache <prefix>
  ```

- CSCug58617

  Symptom: Usernames do not show up in CCP Express. Username shows up on a router with default configuration.

  Conditions: The symptom is observed on routers with configurations that break show runn | format.

  Workaround: Use default configuration.

- CSCug58977

  Symptom: 2.6Gbp/s traffic is observed on both of the VPN SPA interfaces. Traffic direction: Rx on outside interface, Tx on inside interface.

  Conditions: This symptom occurs when fragmented IPSec packet arrives on clear side. The issue is observed only in VRF mode.

  Workaround: Reload the IPSec card.

- CSCug59746

  Symptom: A crash is seen on the RP in the SS manager process:

  ```
  Exception to IOS Thread: Frame pointer 0x7F58BB22FE80, PC = 0x7C505FB
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SSS Manager -Traceback=
  1#980611ad3b9665cd80fe5178bcd6036a :400000+78505FB :400000+7C68774 :400000+7C6871A
  :400000+1C13522 :400000+7852194 :400000+78512C8 :400000+7C68774 :400000+7C6871A
  :400000+33A8AC1 :400000+77DD92F :400000+33C3E4C :400000+33AFE89 :400000+33B2564
  :400000+7824301 :400000+7823F37 :400000+77FA27F
  ```

  Conditions: The issue appears to be related to NAS port. It looks like a key is being set when the issue occurred. The exact conditions are still being investigated.

  Workaround: Possibly remove radius or more specifically, NAS port configurations. This still needs to be verified.

- CSCug61485

  Symptom: The Cisco ASR 1000 RP crashes in RSVP.

  Conditions: This symptom occurs when “mpls traffic-eng tunnels” is configured on an interface and “ip rsvp bandwidth” is not configured and the bandwidth on the physical interface is changed.

  Workaround: There is no workaround.

- CSCug62154

  Symptom: CPU shoots to 100% with TACACS configuration. VTY to the device does not work due to this.

  Conditions: This symptom is observed when the router or switch is booted up with TACACS configurations and the CPU shoots up to 100%. Telnet to the router is not possible. Any command issued on the console would take lot of time.

  Workaround: Remove the TACACS configurations and then reboot the router.

- CSCug63013

  Symptom: A DMVPN spoke router running Cisco IOS Release 15.2(4)M3 and configured with “if-state nhrp” might not re-form eigrp neighbourship if the line protocol on the interface goes down and comes back automatically.

  Conditions: This symptom occurs in a DMVPN spoke router running 15.2(4)M3 with “if-state nhrp" configured and interface line protocol going down. It must also be using the new multicast code (15.1(4)M onwards).

  Workaround:

  - Removing “ip nhrp map multicast x.x.x.x y.y.y.y” and readding it resolves the problem.
  - Shut/no shut on the tunnel interface

- CSCug63839

  Symptom: The Cisco 7301 router running c7301-advipservicesk9-mz.152-4.M3 experiences a memory leak in the Crypto IKMP process particularly on the crypto_ikmp_config_send_ack_addr function.

Conditions: This symptom occurs when running the Cisco 7301 router and connecting EasyVPN through it.

Workaround: Reload the router over a period of time.

- CSCug68193

  Symptom: Multicast traffic across ES+ cards stop flowing across subinterfaces.

  Conditions: The symptom is observed after a linecard OIR. After the linecard comes up, multicast traffic stops flowing across subinterfaces.

  Workaround: Shut/no shut the subinterface.

- CSCug69253

  Symptom: Users will see the following error message on unconfiguring a port-map of a protocol:

  ```
  % NBAR Error: Specified port(s) are associated with <protocol-name>
  ```

  Conditions: This symptom occurs when users have port-mapped a protocol on which other protocols are dependant, and this port-map configuration includes the well-known port as well. On unconfiguring this port-map configuration, the error message will be shown.

  For example, a lot of protocols are dependant on http (share-point, youtube, skype, etc.) because they run over http. If the user port-maps http and includes its well-known port (80) in the configuration, then the following error message will be shown during unconfiguration:

  ```
  Router(config)#no ip nbar port-map http tcp 80 94 8080 3128 8092
  % NBAR Error: Specified port(s) are associated with share-point
  ```

  Workaround: Users will not be able to remove this port-map configuration. To revert back, reconfigure http to its original configuration (tcp 80), save the configuration, and reload the router

  The following is the CLI to reconfigure http to its well-known configuration:

  ```
  Router(config)#ip nbar port-map http tcp 80
  ```

- CSCug72891

  Symptom: EIGRP neighbor flaps due to EIGRP SIA. Troubleshooting shows that a race condition causes EIGRP successor loop first and it leads to EIGRP QUERY loop resulting in the neighbor flaps.

  Conditions: The issue is observed when a worse metric update is received from the successor, once the route is already in active state, in a partially peered multiaccess network.

  Workaround: There is no workaround.

- CSCug78098

  Symptom: Supervisor engine crashes and the Cisco IOS software is forced to reload due to PIM process.

  Conditions: This symptom is observed when using the command, **show ip pim rp-hash** right after the BSR RP times out, causes the crash.

  Workaround: Perform these steps in the following order:

  1. Wait for a minute after BSR RP times out before using this command.
  2. Configuring **no ip domain lookup** will make the time taken to execute **show ip pim rp-hash** to a few milliseconds. This will prevent the crash from being reproduced manually.

- CSCug78929

  Symptom: Packets of a certain protocol are dropped due to v6 PACL applied on a switch port.

Conditions: This symptom occurs when v6 PACL contains explicit protocol entries such as “permit 89 any any”.

Workaround: There is no workaround.

- CSCug85947

  Symptom: OSPFv3 routes go missing after an NSR switchover.

  Conditions: This symptom occurs after an SSO.

  Workaround: Clear the IPv6 OSPF process.

- CSCug94275

  Symptom: ES+ card crashes with an unexpected exception to CPU: vector 200, PC = 0x0.

  Conditions: The symptom is observed on the ES+ series linecards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCuh07349

  Symptom: A Cisco 7600 Sup may crash due to SP memory corruption.

  Conditions: This issue is observed on an REP enabled router, which is part of an REP segment. The exact trigger for this issue is not clear.

  Workaround: There is no workaround.

- CSCuh07657

  Symptom: VRF Aggregate label is not re-originated after a directly connected CE facing interface (in VRF) is shut down.

  Conditions: This symptom occurs in an MPLS VPN set-up with Cisco 7600(PE) Router running on Cisco IOS Release 12.2(33)SRE4 with per VRF aggregation.

  For example:

  ```
  mpls label mode vrf TEST protocol all-afs per-vrf
  ```

  Workaround: Downgrade to Cisco IOS Release 12.2(33)SRE3 or earlier.

- CSCuh16115

  Symptom: With VPLS configuration with IP-FRR, on doing multiple churns SP/LC may crash.

  Conditions: The issue occurs when xconnect internal data structre is to be freed up and IP FRR is still pointing to it.

  Workaround: Remove IP-FRR configuration before unprovisioning xconnect.

- CSCuh16927

  Symptom: Mac entries learned on a trunk link are flushed after removing VLANs.

  Conditions: The symptom is observed when some allowed VLANs are removed on a trunk link, all mac address entries learned on this link are flushed. This is issue is specific to extended VLAN IDs.

  Workaround: Executing ping to destination IP after removing VLANs will recover this condition.

- CSCuh21740

  Symptom: There is a deletion and addition of VRFs with MVPNV6 configurations.

  Conditions: This symptom occurs when PIM VRF neighbors are not up.

  Workaround: Reload the router.

- CSCuh24040

  Symptom: BGP routes are not marked Stale and considered best routes even though the BGP session with the peer is torn down. A hard or soft reset of the BGP peering session does not help.

  For BFD-related triggering, the following messages are normally produced with the BGP-5-ADJCHANGE message first, and the BGP_SESSION-5-ADJCHANGE message second. Under normal conditions, the two messages will have identical timestamps. When this problem is seen, the order of the messages will be reversed, with the BGP_SESSION-5-ADJCHANGE message appearing first, and with a slightly different timestamp from the BGP-5-ADJCHANGE message. In the problem case, the BGP_SESSION-5-ADJCHANGE message will also include the string "NSF peer closed the session"

  For example when encountering this bug, you would see:

  ```
  May 29 18:16:24.414: %BGP_SESSION-5-ADJCHANGE: neighbor x.x.x.x IPv4 Unicast vpn vrf
  VRFNAME topology base removed from session NSF peer closed the session May 29
  18:16:24.526: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME Down BFD adjacency
  down
  ```

  Instead of:

  ```
  May 29 18:16:24.354: %BGP-5-ADJCHANGE: neighbor x.x.x.x vpn vrf VRFNAME Down BFD
  adjacency down May 29 18:16:24.354: %BGP_SESSION-5-ADJCHANGE: neighbor x.x.x.x IPv4
  Unicast vpn vrf VRFNAME topology base removed from session BFD adjacency down
  ```

  Log messages associated for non-BFD triggers are not documented.

  Conditions: This symptom is observed when BGP graceful restart is used in conjunction with BFD, but it is possible (but very low probability) for it to happen when BGP graceful restart processing happens when any other type of BGP reset (eg: clear command) is in progress.

  Affected configurations all include: router bgp ASN ... bgp graceful-restart ...

  The trigger is that BGP exceeds its CPU quantum during the processing of a reset, and gives up the CPU, and then BGP Graceful Restart processing runs before BGP can complete its reset processing. This is a very low probability event, and triggering it is going to be highly dependent on the configuration of the router, and on BGP's CPU requirements.

  It is not possible to trigger this bug unless BGP graceful-restart is configured.

  Workaround: If you are engaged in active monitoring of router logs, and the bug is being triggered by a BFD-induced reset, you can detect this situation by watching for the reversal of log message order described in the Symptoms section, and then take manual steps to remedy this problem when it occurs.

  On the problematic router, issue **no neighbor <xxx> activate** command under the proper address-family will clear the stale routes.

  The other option is to manually shutdown the outgoing interface which marks the routes as "inaccessible" and hence not been used anymore. This prevents the traffic blackhole but the routes will stay in the BGP table.

  More Info: This bug affects all releases where CSCsk79641 or CSCtn58128 is integrated. Releases where neither of those fixes is integrated are not affected.

- CSCuh27770

  Symptom: On a dual-RP system which is configured for stateful switchover (SSO), some VPLS virtual circuits may fail to be provisioned on the standby route processor.

  Conditions: This symptom is observed when the VFI consists of VLAN interfaces that are also configured for IP.

  Workaround: Reload the standby RP.

- CSCuh29716

  Symptom: When a call is transferred from IVR to PSTN, the codec negotiation with Verizon fails only if the original invite received includes fax capabilities, dropping the call with reason code 47 and hanging the UDP port used.

  Call flow:

  ```
  Verizon -- CUBE -- CUSP -- Genesys/IVR, transferred with SIP Refer back to PSTN
  hair-pinning the call on CUBE.
  ```

  All subsequent calls that try to re-use the same UDP port for RTP stream are dropped with reason code 47 and provisn RSP fail is logged on show voip fpi stats.

  Conditions: This symptom occurs in hair-pinned calls that receive FAX capabilities on the original SIP invite from Verizon.

  Workaround: There is no workaround. Reload the router to clear UDP ports.

- CSCuh32177

  Symptom: The **no passive-interface** <*if-name*> command will be added automatically after configuring the **ipv6 enable** command on the interface even though the **passive-interface default** command is configured for OSPFv3.

  ```
  --- (config)#interface FastEthernet0/2/0 (config-if)#ipv6 enable (config-if)#end
  #sh run | sec ipv6 router ospf ipv6 router ospf 100 router-id 10.1.1.1
  passive-interface default no passive-interface FastEthernet0/2/0 <<< Added
  automatically. ---
  ```

  Conditions: This symptom occurs when the **passive-interface default** command is configured for OSPFv3.

  Workaround: Adjust the configuration manually. In this example it would be “passive-interface FastEthernet0/2/0”.

- CSCuh40275

  Symptom: SNMP occupies more than 90% of the CPU.

  Conditions: This symptom is observed when polling the cefFESelectionTable MIB.

  Workaround:Execute the following commands:

  ```
  snmp-server view cutdown iso included
  snmp-server view cutdown cefFESelectionEntry excluded
  snmp-server community public view cutdown ro
  snmp-server community private view cutdown rw
  ```

- CSCuh40329

  Symptom: OSPFV3 runs as PE-CE, but used to learn IPv4 prefixes. Core facing interface is GRE tunnel where OSPF and LDP runs. OSPV3 based Shamlinks are created between PEs. When tunnel flaps , OSPF and LDP recovers, but in a few seconds tunnel locks up. In locked up condition, all traffic fails on the tunnel, even directly connected pings. The only way to recover is to reconfigure the tunnel from scratch. It happens fairly consistently after every re-convergence, not every time though.

  Conditions: This symptom is seen only on ISRG2s that are configured as PEs. They are so far seen with 3925 running Cisco IOS Release 15.3(2)T and 2911 running Cisco IOS Release 15.2(4)M3.

  Workaround: Use OSPF V2 based shamlinks.

- CSCuh40617

  Symptom: Ping fails when “encap dot1q” is configured on an FE SPA inserted in bay 1 of flexwan.

Conditions: This symptom is observed when FE SPA is inserted in bay 1 of flexwan.

Workaround: Move the SPA to bay 0 of flexwan.

- CSCuh43027

  Symptom: Prefixes withdrawn from BGP are not removed from the RIB, although they are removed from the BGP table.

  Conditions: A withdraw message contains more than one NLRI, one of which is for a route that is not chosen as best. If deterministic med is enabled, then the other NLRI in the withdraw message might not eventually be removed from the RIB.

  Workaround: Forcibly clear the RIB.

- CSCuh43252

  Symptom: After upgrading to Cisco IOS Release 15.0(2)SE3, you can no longer authenticate using TACACS. The TPLUS process on the switch will be pushing the CPU up to 99%.

  Conditions: The symptom is observed when you use TACACS for authentication.

  Workaround: Downgrade the switch to a version prior to Cisco IOS Release 15.0(2)SE3.

- CSCuh43255

  Symptom: The BGP task update-generation process may cause the router to reload, in a rare timing condition when there is prefix flap and there is high scale of prefixes going through update-generation, including the flapping prefix.

  Conditions: The symptom is observed when the Cisco ASR router is acting as a route server for BGP along with having various route-server contexts. The router does not do any forwarding. It merely processes control plane traffic.

  Workaround: There is no workaround.

  More Info: The setup is the same as mentioned in this doc: http://www.cisco.com/en/US/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_route_server_xe.html.

- CSCuh46031

  Symptom: The Cisco ASR 1000 router sends a different Acct-Session-Id in the Access-Request and Accounting-Request for the same user.

  Conditions: This symptom occurs when Flex VPN IPsec remote access is configured.

  Workaround: There is no workaround.

- CSCuh46849

  Symptom: A Cisco ASR 1000 router may display the following log with a traceback:

  ```
  SCHED-3-UNEXPECTEDEVENT Process received unknown event (maj 80, min 0).
  ```

  Conditions: The conditions are unknown.

  Workaround: Reload the router.

- CSCuh48840

  Symptom: Cisco Router crashes.

  Conditions: This symptom is observed under the following conditions:

  - sup-bootdisk formatted and copied with big size file, like copy 7600 image file around 180M size

- reload box, and during bootup try to write file to sup-bootdisk (SEA write sea_log.dat 32M bytes)
- then the issue appear
- When the issue seen, check the sea_log.dat always with 0 byte
- No matter where (disk0 or bootdisk) to load image.
- No matter sea log disk to sup-bootdisk or disk0:. I reproduced the issue with “logg sys disk disk0:” config.

```
SEA is calling IFS API to create sea_log.dat, looks like IFS creating file hungs SP.
sea_log.c : sea_log_init_file() -> ifs_open() -> sea_zero_log() -> ifs_lseek() ->
ifs_write()
```

Workaround: There is no workaround.

- CSCuh53544

  Symptom: OSPF ABR router does not flush type-4 ASBR summary LSA after NSR swithover if the connection to ASBR is lost during NSR switchover.

  Conditions: This symptom is occurs when the VSS system acts as ABR and loses connection to an ASBR during NSR switchover. This configuration is not recommended and Layer 3 topology should not change during the switchover.

  Workaround: Clear ip ospf proc.

- CSCuh56327

  Symptom: IP SLA responder crash occurs on Cisco ASR 1002 router in Cisco IOS Release 15.2(4)S, Cisco IOS Release 15.2(4)S1, and Cisco IOS Release 15.2(4)S2.

  Conditions:This symptom occurs when ip sla udp jitter with precision microseconds, udp jitter with milliseconds and udp echo are configured on the sender device with the same destination port on Cisco ASR 1002 router.

  Workaround:Use different destination ports for udp-echo and udp jitter with millisecond precision than udp jitter with microsecond and optimize timestamp.

- CSCuh62266

  Symptom: During normal operation, the Cisco ASR 1000 router may crash after repeated SNMP related watchdog errors.

```
Jun 15 2013 10:43:30.325: %SCHED-0-WATCHDOG: Scheduler running for a long time, more
than the maximum configured (120) secs. -Traceback= 1#6d024ee43b83b4f5539a076aa2e8d467
:10000000+56A5348 :10000000+20F7D54 :10000000+2513910 :10000000+20F807C
:10000000+20EBE84 :10000000+2119BA8 :10000000+20EBE84 :10000000+2106C24
:10000000+20EBE84 :10000000+213C9E8 :10000000+213CC34 :10000000+225B748
:10000000+222941C :10000000+2214314 :10000000+224812C -Traceback=
1#6d024ee43b83b4f5539a076aa2e8d467 :10000000+21416F0 :10000000+2513910
:10000000+20F807C :10000000+20EBE84 :10000000+2119BA8 :10000000+20EBE84
:10000000+2106C24 :10000000+20EBE84 :10000000+213C9E8 :10000000+213CC34
:10000000+225B748 :10000000+222941C :10000000+2214314 :10000000+224812C
```

  Conditions: This symptom occurs while trying to obtain data from IP SLAs Path-Echo (rttMonStatsCollectTable) by SNMP polling operation.

  Workaround: There is no workaround other than to disable SNMP configuration from the router.

  More Info: This crash occurred in a customer environment and device with a particular version of the software (Cisco IOS Release 15.1(2)S2). No other similar issue has been identified so far.

- CSCuh78146

  Symptom: ES+ LC crashes while sending L2 traffic from Ixia.

  Conditions: This symptom occurs while sending continuous traffic from Ixia. The ES+ interface has the configurations of EVC and BD.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S3a

Cisco IOS Release 15.2(4)S3a is a rebuild release for Cisco IOS Release 15.2(4)S. The caveats in this section are resolved in Cisco IOS Release 15.2(4)S3a and Cisco IOS Release 15.2(4)S3 but may be open in previous Cisco IOS releases.

- CSCuf64313

  Symptoms: Linecard crash is seen with machine-check exception.

  Conditions: There is no trigger. The crash is random.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S3

Cisco IOS Release 15.2(4)S3 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveats in this section are resolved in Cisco IOS Release 15.2(4)S3 but may be open in previous Cisco IOS releases.

- CSCsr06399

  Symptoms: A Cisco 5400XM may reload unexpectedly.

  Conditions: This symptom is intermittent and is seen only when the DSPs available are insufficient to support the number of calls.

  Workaround: Ensure that sufficient DSPs are available for transcoding.

- CSCtx50235

  Symptoms: During a crash on the Cisco Catalyst 6500, the normal crash information from the crashinfo files may be missing due to the crashes showing the Routing processor (RP) being reset by the Switching Processor (SP) and the RP crashinfo also showing the RP being reset by the SP. This bug addresses this serviceability issue and it has nothing to do with the root cause of the crash itself.

  In a majority of cases, the crash has been a single-event crash and has not repeated.

  Conditions: Conditions of this symptom are not known currently. At this point, it is believed that the real fault of the crash belongs to the SP.

  Workaround: There is no workaround.

- CSCty07538

  Symptoms: TCP sessions get reset intermittently when NAT is configured with more than 1500 translations.

  Conditions: This symptom occurs in the Cisco Catalyst 6500-Sup720/Sup32 when NAT is configured with more than 1500 translations.

  Workaround 1: Remove NAT.

Workaround 2: Force packets coming to RP on the NAT interfaces to be process switched by configuring **no ip route-cache** on the NAT interfaces.

- CSCtz26779

  Symptoms: A 7600 ES line card and/or SUP/RSP may crash displaying DATACORRUPTION-1-DATAINCONSISTENCY messages.

  Conditions: This symptom is observed when a policy-map is configured where the name exceeds 80 characters. This will trigger DATACORRUPTION messages on ES line cards and might cause the SUP/RSP to crash as well.

  Workaround: Configure policy-map names that are less then or equal to 80 characters.

- CSCtz53214

  Symptoms: The “clear counter pseudowire <#>” commands do not clear the pseudowire specific counters.

  Conditions: This symptom is reported to be present in all Cisco IOS Release 15.X(S) versions.

  Workaround: Issuing global clear count (“clear counters”) will clear counters including pseudowire specific counters.

- CSCtz60398

  Symptoms: Continuous “platform assert failure” trace backs with CFM over Xconnect on the box occurs.

  Conditions: This symptom occurs with CFMoXconnect and MPLS TE in the core. Flap the core-facing link.

  Workaround: There is no workaround.

- CSCtz97197

  Symptoms: SIP SPAs go in the out of service state in a scaled subinterface configuration (more than 2000 subinterfaces on a single Gigabit Ethernet port).

  Conditions: This symptom occurs while performing ISSU between the iso1-rp2 and iso2-rp2 Cisco IOS XE Release 3.6S throttle image. After ISSU runversion, the SIP SPAs go in the out of service state. This issue is seen in a heavily scaled configuration. The issue is observed when there are 2000 to 3000 subinterfaces on a single SPA and the following limits are exceeded:

  ```
  Overall Dual stack VRFs per box: 2800 Dual stack limit on interface: 1000
  ```

  Workaround: This issue is not seen in the following scenario:

  1. Before doing a load version from RP0(initial active), enter the following command:

     ```
     asr1000# show ipv6 route table | inc IPv6
     ```

  2. Note down the number of IPv6 route tables in the system.
  3. Do a load version.
  4. Wait for standby to come up to Standby hot.
  5. Enable the standby console from RP0 (active).

     ```
     asr1000#configure terminal
     Enter configuration commands, one per line. End with CNTL/Z.
     asr1000(config)#
     asr1000(config)#redundancy
     asr1000(config-red)#main-cpu
     asr1000(config-r-mc)#standby console enable
     ```

  6. Log in to the standby console and enter the following command:

```
asr1000-stby# show ipv6 route table | inc IPv6
```

7. Then, note down the number of IPv6 route tables in standby. If the number is lesser than the number noted in step 2, wait for some time and reverify till it reaches the number noted in step 2.
8. Issue ISSU runversion from RPO(active).

- CSCua43781

  Symptoms: WCCP redirection does not work. The mls netflow table does not get installed in the Cisco Catalyst 6500 switches for packets to get redirected to the WAAS hardware.

  Conditions: This symptom occurs when the current configuration, MASK/GRE/GRE, is changed to HASH/L2/L2.

  Workaround: Perform shut/no shut once or twice on the interface connected to the WAE hardware.

- CSCub10950

  Symptoms: The router crashes when an MR-APS switch is made. The crashes occur randomly.

  Conditions: This symptom occurs when the MLP is configured with 12 links.

  Workaround: There is no workaround.

- CSCub12911

  Symptoms: The Cisco ASR Series routers crash if the AAA profile is not defined and a DHCP discover message is sent from MN to MAG/ISG.

  Conditions: This symptom occurs when the AAA profile is not defined.

  Workaround: Define the AAA profile in ISG.

- CSCub28997

  Symptoms: Overlord crashes with 2000 crypto sessions (4000 IPSec SAs) upon repeatedly clearing and reestablishing the SAs.

  Conditions: This symptom is observed when the box is configured with 1K VRFs and 1K Virtual templates, and the crypto sessions are repeatedly cleared or reestablished.

  Workaround: There is no workaround.

- CSCub45763

  Symptoms: The device crashes due to SYS-2-FREEFREE and SYS-6-MTRACE messages while a CDP frame is being processed.

  Conditions: This symptom occurs when CDP is in use.

  Workaround: Disable CDP using the **no cdp run** command.

  Note: If the device in question relies on or supports a phone or voice network, this is not a valid workaround.

- CSCub56064

  Symptoms: Ping fails after doing EZVPN client connect if CEF is enabled.

  Conditions: This symptom is observed with the Cisco IOS Release 15.3(0.8)T image. This issue is seen only for a specific topology, where the in/out interface is the same.

  Workaround: There is no workaround.

- CSCub56842

  Symptoms: The router stops passing IPsec traffic after some time.

Conditions: This symptom is observed when the **show crypto eli** command output shows that during every IPsec P2 rekey, the active IPsec-Session count increases, which does not correlate to the max IPsec counters displayed in SW.

Workaround: Reload the router before active sessions reach the max value.

To verify, do as follows:

```
router#sh cry eli
CryptoEngine Onboard VPN details: state = Active
Capability: IPPCP, DES, 3DES, AES, GCM, GMAC, IPv6, GDOI, FAILCLOSE, HA
IPSec-Session: 7855 active, 8000 max, 0 failed <<<
```

- CSCub58119

  Symptoms: VRF-aware GRE tunnel traffic drops while performing SSO(VRF-GRE tunnel adjacency is wrong after performing SSO).

  Conditions: This symptom occurs because of incorrect programming of the adjacency interface.The adjacency information on the standby is incorrect as it does not get synced from “active”. Configure VRF-aware GRE tunnels and send traffic to all the tunnels. Perform SSO and traffic drops on all the tunnels.

  Workaround: Reload the router or perform shut/no shut on the tunnels.

- CSCub60422

  Symptoms: The ME-3600X-24CX-M box crashes on executing the **diagnostic start test all** command.

  Conditions: This symptom occurs on executing the **diagnostic start test all** command.

  Workaround: There is no workaround.

- CSCub72198

  Symptoms: Executed CLI fails to sync to standby and results in standby reload.

  Conditions: This occurs when the following conditions are met:

  1. Active and standby are running different version of IOS image.
  2. The CLI being applied is not PRC compliant, meaning that this CLI does not return a valid parser return code.

  Workaround: Avoid applying CLIs that are not PRC compliant during image upgrade or downgrade.

- CSCub85416

  Symptoms: The router crashes after the ISSU RUN VERSION in the latest mcp_dev image with G8302 configurations.

  Conditions: This symptom occurs with 11k EoMPLS VC and G8302 configurations.

  Workaround: There is no workaround.

- CSCub93442

  Symptoms: FlexVPN client does not get assigned with IPv6 address when IPv6 address is assigned using radius attribute “addrv6”.

  Conditions: This symptom is observed on assigning IPv6 using the radius attribute “addrv6”.

  Workaround: Assign IPv6 address statically or use radius IPv6 pool attribute “ipv6-addr-pool”.

  Further Problem Description:

  1. Radius Server is used for assigning IPv6 address to the FlexVPN clients.

2. Using radius attribute “ipv6-addr-pool” for assigning IPv6 address from a Ipv6 pool defined works fine.
3. If Radius attribute “addrv6” is used to assign IPv6 address then the IPv6 address assignment fails and client sends notification with internal address failure.

- CSCuc05929

  Symptoms: After a reload, sometimes the MPLS forwarding function on some interfaces is not enabled. Some interfaces that were configured with “mpls ip” and link-state-up do not show with the **show mpls interface** command. This issue depends on a timing of the interface up.

  Conditions: Sometimes the issue occurs after a router reload or SIP/SPA reload. It is not affected when you configure “mpls ip” on an interface, admin-shutdown/no shutdown, and link-flap.

  Workaround: There is no workaround. When the issue occurs, do an admin-shutdown/no shutdown on the affected interface or disable/re-enble MPLS on the interface.

- CSCuc21610

  Symptoms: The console displays a message indicating that offloading is not supported for the BFD echo mode.

  Conditions: This symptom occurs when a BFD session is configured in the echo mode.

  Workaround: There is no workaround. The issue has no functionality impact.

- CSCuc23542

  Symptoms: The PXE client network boot fails when an ME3600-running 152-4.S is the DHCP relay agent.

  Conditions: This symptom occurs when the ME3600 changes the option 54 “DHCP Server Identifier” address to its own IP address in the DHCP Offer received from the PXE DHCP server. This causes the client to send the PXE boot request (port 4011) to the ME3600 instead of the PXE server.

  Workaround: Downgrade ME3600 to Cisco IOS Release 15.1(2)EY.

- CSCuc31761

  Symptoms: The router crashes when GDOI groups are removed.

  Conditions: This symptom occurs when the “crypto isakmp diagnose error <no>” CLI is enabled. This CLI is now enabled by default.

  Workaround: Remove or disable the **crypto isakmp diagnose error** command.

- CSCuc43719

  Symptoms: The Cisco ASR 903 router with dual RSP may crash.

  Conditions: This symptom occurs with configurations related to NBAR. There is no specific trigger for this symptom.

  Workaround: Do not have any NBAR configurations on the box as these are not supported on the Cisco ASR 903 router.

- CSCuc54300

  Symptoms: During an SSO or an initial bootup, standby fails and reboots again.

  Conditions: This symptom occurs when a reload or SSO is performed.

  Workaround: There is no workaround.

- CSCuc54604

  Symptoms: CUBE SP does not respond to any SIP messages sent across using TCP. Call Flow:

```
Multiple CUCM's ---> SIP --->CUBE SP--->Provider
```

Conditions: This symptom occurs in the Cisco IOS Release 15.2(01)S01 and is only active when there are calls running SIP TCP. During create/close transaction on TCP, the control buffer will be on hold. So if closing of the existing TCP connection is needed while the control buffers are all being held, the connection will be marked as dead and will not be able to notify the corresponding peer. Therefore, the peer might still send data through that connection which CUBE-SP would think as invalid and get dropped internally.

Workaround: Send the SIP call as UDP instead of TCP.

- CSCuc59386

  Symptoms: Continuous IOMD crashes occur on OC-3 IM. Interfaces on OC-3 IM are not configurable and the following error message is seen:

  ```
  stand-by does not support this command
  ```

  Conditions: This symptom is seen on an HA Cisco ASR 903 router setup with OC-3 IM. It is observed when an IOMD crash happens on an active RSP and the standby IOMD session handle is not cleared.

  Workaround: Reload the standby RSP.

- CSCuc78328

  Symptoms: SP crashes followed by an RP reset.

  Conditions: This symptom occurs when multicast-enabled (PIM) tunnels are protected with IPSec.

  Workaround: There is no workaround.

- CSCuc85319

  Symptoms: RP crashes during the TFTP ATM interface configuration.

  Conditions: This symptom occurs after flapping the ATM subinterface configured with the ATM bundle 8192 times.

  Workaround: There is no workaround.

- CSCuc93082

  Symptoms: A Bulk Sync failure occurs.

  Conditions: This symptom occurs when the standby is brought up from ROMmon and the **service-policy** command is configured on the CEM circuit as active.

  Workaround: There is no workaround.

- CSCuc96345

  Symptoms: ARP exchange between the Cisco 7600 and the client device fails. The Cisco 7600 has an incomplete ARP entry in its ARP table for the client. This issue is likely to be seen between the Cisco 7600 and other Cisco platforms with MAC address 6073.5Cxx.xxxx. The incoming ARP reply is parsed by the platform CEF as an IP packet and dropped.

  The following OUIs (as of October 30, 2012) are affected: (first 3 bytes from MAC address/MAC starts with)

  ```
  14-73-73 20-73-55 4C-73-67 4C-73-A5 54-73-98 60-73-5C (One of Cisco's OUI ranges)
  64-73-E2 70-73-CB 8C-73-6E 98-73-C4 A0-73-32 C4-73-1E D0-73-8E F0-73-AE F4-73-CA
  ```

  Conditions: This symptom is observed with the EVC pseudowire and 802.1q subinterface on the same physical interface, and connectivity via the subinterface is affected.

  Sample configuration:

```
interface TenGigabitEthernet3/1 service instance 2013 ethernet encapsulation dot1q 411
second-dot1q 200 rewrite ingress tag pop 2 symmetric xconnect 10.254.10.10 3350075
encapsulation mpls interface TenGigabitEthernet3/1.906 encapsulation dot1Q 906 ip
address 10.10.10.1 255.255.255.0
```

Workaround: - There should be a static ARP entry on the Cisco 7600 for the client's MAC and IP. - Change the MAC address of client to a nonaffected OUI.

NOTE: This DDTS is caused or exposed due to fix of CSCtc22745.

- CSCuc96631

  Symptoms: Incoming calls through e1 r2 stop working in Cisco IOS Release 15.2(4)M1.

  Conditions: This symptom is observed with incoming calls through e1 r2 in Cisco IOS Release 15.2(4)M1. Outgoing calls work fine.

  Workaround: Use Cisco IOS Release 15.2(2)T.

- CSCud01502

  Symptoms: A crash occurs in CME while accessing a stream in sipSPIDtmfRelaySipNotifyConfigd.

  Conditions: This symptom occurs in CME.

  Workaround: There is no workaround.

- CSCud03250

  Symptoms: Large TCP data transfers take longer than expected (about a 40% increase in time). In particular, initial BGP convergence for a full internet routing table after reload is known to increase by several minutes. Performance degradation was seen starting the XE37 throttle build 09/18 (BLD_V152_4_S_XE37_THROTTLE_LATEST_20120918_070025).

  A comparison of sniffer traces of affected and unaffected traffic will show that in impacted versions of Cisco IOS, TCP more frequently probes the path MTU, and that when the larger packets are dropped, it treats these drops as indicating the presence of network congestion, and slows down the rate of data transmission.

  Conditions: This symptom is observed when the user tries with the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120917_070015 label and the performance number is still good, but the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120918_070025 label image shows much higher performance numbers in the order of 400 seconds. This issue is seen when the user also tries with the BLD_V152_4_S_XE37_THROTTLE_LATEST_20120917_070015 label.

  Workaround: The underlying problem is caused by changes in the TCP path MTU discovery algorithm. Disable TCP path MTU discovery for affected BGP neighbors. Depending on the release, this is done by configuring the following:

  ```
  neighbor x.x.x.x transport path-mtu-discovery disable or no neighbor x.x.x.x transport
  path-mtu-discovery
  ```

  Note that the use of this workaround may have other negative performance consequences caused by packet fragmentation, and there may be a need to tune interface MSS.

- CSCud05368

  Symptoms: Traffic will be redirected to the WCCP client even when it is denied in the WCCP redirect ACL.

  Conditions: This symptom occurs with WCCP on the Cisco ASR 1000 router, when there are port(s) defined in service definition, for example, 80 for web-cache, while different port(s) defined in permit entries of redirect-ACL.

  ```
  For example: permit tcp any eq 81
  ```

Workaround 1: Move the deny entries before the permits when possible (especially for deny... host ...). But it still may not work in some situations.

Workaround 2: Use different redirect ACLs for each service, and remove the unnecessary ones for specific services (that is, the permit entries with ports not matching service definition).

- CSCud07642

  Symptoms: AAL0 encapsulation fails.

  Conditions: This symptom occurs when “control” is disabled.

  Workaround: There is no workaround.

- CSCud09870

  Symptoms: The device crashes when you enable ?debug cmd-cfm? over xconnect with PC.

  Conditions: This symptom is observed when you configure the CFM over xconnect with PC downmep. After enabling the **debug** command, the device crashes.

  ```
  debug ethernet cfm pm session db 0.
  ```

  Workaround: Issue the **undebug all** command.

- CSCud11627

  Symptoms: SUP720 supervisor module may hang in ROMMON after the module reset triggered by TM_DATA_PARITY_ERROR.

  Conditions: The issue is observed after a module reset triggered by TM_DATA_PARITY_ERROR.

  Workaround: Power off or power on the router.

- CSCud19149

  Symptom: Traffic drops for a few VPLS VCs with ECMP links.

  Conditions: This symptom occurs when one of the ECMP paths is shut and when more than 200 VPLS VCs are configured.

  Workaround: There is no workaround.

- CSCud22038

  Symptoms: When a PC is moved between two VLAN ports (on one port, ISG is enabled and the other port is non-ISG) several times by its LAN cable connection on the L2SW that is connected to the Cisco ASR 1000 router, the PC is unable to receive DHCP OFFER due to the wrong VLAN ID from the DHCP server on the Cisco ASR 1000 router.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(4)S1.

  Workaround: There is no workaround.

- CSCud24601

  Symptoms: After performing an SSO on a Quad-SUP setup, the previous standby displays the following error message on the console:

  ```
  *Nov 16 15:50:28.455: SW1-7_STBY: ics_cs_nego_open_active_port: ERROR: (no such port): Failed to locate active port *Nov 16 15:50:29.591: SW1-7_STBY: Bring up standby supervisor as a DFC *Nov 16 15:50:32.331: %PFREDUN-SW1-7_STBY-6-STANDBY: Initializing for SSO mode in In-chassis Domain
  ```

  Conditions: This symptom occurs occasionally after performing an SSO on a Quad- SUP setup. This error message is harmless. The system will still reach SSO successfully.

  Workaround: There is no workaround.

- CSCud28541

  Symptoms: SP crashes on doing **no mpls ip** followed by **shut** on port-channel acting as core link for scaled VPLS and EoMPLS setup.

  Conditions: In case of VPLS going over port-channel protected by IP-FRR, when the port-channel is shut the AToM VC is going down and getting created again. Also the PPO object is getting created afresh. The VC going down is not handled for VPLS case and AToM VC's pointer are still stored in IP-FRR's EoMPLS list which is getting access and hence crashing.

  Workaround: There is no workaround.

- CSCud30806

  Symptoms: Policy with class map match-all with prec 1 and prec 2 is accepted for WRED.

  Conditions: Conditions to this symptom are not known currently.

  Workaround: There is no workaround.

  Further Problem Description: match-all should not accept two prec values.

  ```
  class-map match-all prec1_2 match precedence 1 match precedence 2
  ```

- CSCud41058

  Symptoms: There is a route-map which matches tags and set a new value. This route-map is used in an EIGRP outbound distribute list. One in 10 times based on the received route tag, the correct route tag value is not set while advertising out.

  Conditions: The symptom is observed when you use a route map which matches tags and sets a new tag. Used in **distribute-list route-map** *name* **out**.

  Workaround: Clear the EIGRP process or readvertise the route.

- CSCud46309

  Symptoms: When an SSO is configured and a GR full mode is not configured, TE tunnels may stay down after a switchover.

  Conditions: This symptom is observed under the following conditions:

  - When SSO is configured.
  - When GR full mode not configured.
  - When a switchover is performed.

  Workaround: There is no workaround.

- CSCud51791

  Symptoms: Memory leak is seen on the router related to CCSIP_SPI_CONTRO.

  Conditions: This symptom is observed in CME SIP phones with Presence in running-configuration.

  Workaround: There is no workaround. You may try to remove Presence from running-configuration.

- CSCud56281

  Symptoms: There is a memory corruption issue while loading an NBAR protocol pack.

  Conditions: This symptom occurs when an NBAR protocol pack is loaded onto the router using the **ip nbar protocol-pack** command.

  Workaround: There is no workaround.

- CSCud63381

  Symptoms: Switching from periodic to on-demand DPDs may cause the DPDs to fail intermittently and thus IPSEC Failover may not work correctly.

  Conditions: This symptom is observed under the following conditions:

  1. If you are using Cisco 7200-VSA.
  2. For Cisco IOS Release 15.1(4)M2.
  3. When on-demand DPDs are configured for IPSEC Failover.

  Workaround: Disable the SCTP session:

  ```
  ipc zone default association 1 shutdown
  ```

- CSCud64870

  Symptom: DMVPN hub ASR1004 may crash after fetching the CRL from MS CRL server.

  Conditions: The crash occurs when there are 5 CDPs for the hub router to fetch the CRL. Since there are multiple CDPs, the hub router fetches the CRL in a parallel way, which leads to a crash under a timing issue.

  Workaround: Setting up one CDP instead of multiple CDPs will avoid the timing condition that leads to the crash.

- CSCud66955

  Symptoms: SPA-2CHT3-CE-ATM is flapping with Nortel Passport due to the fast bouncing of up or down 10s, after the interface is brought up.

  Conditions: This symptom is observed in E3 and DS3 mode.

  Workaround: There is no workaround.

- CSCud67105

  Symptoms: Virtual-Access is not removed when “clear ip nhrp” or “clear crypto session” are issued or when spoke-spoke FlexVPN session is gone. This is seen only in case of FlexVPN.

  Conditions: This symptom is seen only when CSCuc45115 is already in image.

  Workaround: There is no workaround.

- CSCud68830

  Symptoms: End to end L3 traffic is affected if the host queue (cpu queue 2) increments continuously at high rates (2000 packets and above).

  Conditions: This symptom occurs when the host queue (cpu queue 2) increments continuously at high rates (2000 packets and above).

  Workaround: There is no workaround.

- CSCud69421

  Symptoms: The router crashes continuously after downgrade with mode 3.

  Conditions: This symptom is observed when you set the SDM preferred template to mode 3 and reload with the XE37 image.

  Workaround: After the router crashes, boot with any XE38/mcp_dev image and set the SDM preferred template to mode 4 (mode 2) and boot with the XE37 image.

- CSCud71606

  Symptoms: The LSMPI Tracebacks errors are seen while clearing IP routes multiple times.

Conditions: This symptom is observed under the following conditions:

- Configuring OSPF
- Has more than 1000 OSPF neighbor, which will make OSPF LSU packet get fragmented
- Clear IP OSPF process * and OSPF will send LSU packet, which triggers this error message

>Workaround: There is no workaround.

- CSCud78649

  Symptoms: The following error message occurs when activating SBC:

  ```
  SBC: SBC ^T^U^V not configured
  ```

  Conditions: This symptom is observed when you run the **activate** command just after the **media-address ipv4 ...** command, as shown below:

  ```
  ASR-1001-CCN-7(config)#sbc test ASR-1001-CCN-7(config-sbc)#sbe
  ASR-1001-CCN-7(config-sbc-sbe)#media-address ipv4 1.20.0.2 vrf vrfa
  ASR-1001-CCN-7(config-sbc-media-address)#activate SBC: SBC ^A^T not configured
  ```

  Workaround: Exit SBC first, then enter SBC again and then run the **activate** command.

- CSCud84695

  Symptoms: Serial interface with FRF.12 feature is not coming up.

  Conditions: This symptom is observed when the flags related to FRF.12 feature are not properly updated in Elocal UCODE table.

  Workaround: There is no work around.

- CSCud86240

  Symptoms: The Cisco ASR 1000 ESP crashes (ucode core file created) when compressed packets are sent on a Multilink PPP interface using the Cisco IOS XE 3.5 Release and earlier Cisco ASR 1000 software images. On Cisco IOS XE 3.6 Release and later on Cisco ASR 1000 software images a crash does not occur, but routed traffic on configured interfaces are not forwarded.

  However, local traffic between the peer routers may still be forwarded. In all releases, routed traffic will be dropped on any other interfaces (for example, PPP, Multilink PPP, HDLC, and so on.) configured for this mode of compression.

  Conditions: This symptom is observed if the legacy IOS compression feature compress **[mppc | stac | predictor]** is configured on any interface (for example, PPP, Multilink PPP, HDLC, and so on.).

  If this feature is configured on a Multilink PPP interface then the ESP crash can be encountered if using an Cisco IOS XE 3.5 Release and an earlier Cisco ASR 1000 software image.

  Workaround: Remove the compress **[mppc | stac | predictor]** feature configuration from all interfaces as this functionality is not supported on the Cisco ASR 1000 router. The software fix associated with this bug report will be removing this configuration option from the Cisco ASR 1000 router.

- CSCud90457

  Symptoms: The serial interface of CE interfaces connected to the CEM interfaces on PE remain down on router reload with scaled configuration.

  Conditions: This symptom is observed when you have CESoP and SAToP scaled circuits and perform a router reload.

  Workaround: Perform IM OIR to resolve the issue.

- CSCud96075

  Symptoms: A router running Cisco IOS Release 15.2(4)M2 will reload with a bus error soon after the DSP reloads when there is a live transcoding session.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(4)M2.

  Workaround: There is no workaround.

- CSCud99911

  Symptoms: There may be a delay of 15 seconds or more before switching over to a backup pseudowire in a pseudowire redundancy configuration.

  Conditions: This symptom is observed on the Cisco ME 3600 platform when the attachment circuit is a VLAN.

  Workaround: There is no workaround.

- CSCue00726

  Symptom: There is no functional impact to the system performance, warning messages will be seen only during initialization of the router and there are no security concerns on these units:

  ```
  *Dec 16 17:58:02.432: IOSXE_PLATFORM-3-WDC_INVALID_LENGTH WDC length can not be
  determined: 65535
  *Dec 16 17:58:10.703: PLATFORM_SCC-1-AUTHENTICATION_FAIL Chassis authentication failed
  *Dec 16 17:58:10.703: IOSXE_AUTHENTICATE-2-AUTHENTICATE_FAILED. The platform
  authentication failed
  ```

  Conditions: Programming of Quack & WDC (Watch Dog Certificate) was accidentally disabled in manufacturing during the regression testing. This caused units to ship without Quack & WDC programming. These messages show up at boot up for those specific units that had the quack disabled.

  Workaround: There is no workaround.

  Field Action: Strategy for Field Units:

  - Update Cisco IOS to remove authentication error messages for impacted serial numbers only. This action is In progress.
  - Target code releases with the update include Cisco XE 3.7.3 and Cisco XE3.8.1 and later.
  - TAC teams have the effective serial number list. Customers will be given a choice to upgrade to new Cisco IOS image (availability to be confirmed) or RMA the unit.
  - Customer also have the option to take no action if they want to ignore this message.

- CSCue03316

  Symptoms: The box crashed during scale testing.

  Conditions: During scale testing, the box runs out of memory resulting in MALLOCFAIL. Memory malled is not checked for failure resulting in crash.

  Workaround: There is no workaround.

- CSCue03418

  Symptoms: The OSPF protocol flaps may be noticed on executing the “redundancy force switchover” or on switchover. These are seen very intermittently and can cause about 20 to 30 seconds of traffic loss.

  Conditions: This symptom is observed on SSO or executing the **redundancy force-switchover** command and on a HA system with 6 seconds as OSPF “dead-interval”.

  Workaround: Increase the dead-interval value.

- CSCue05358

  Symptoms: “Collect Identifier mac-address” -- for routed session is not working for the client who roams to a new interface.

  Conditions: This symptom is observed if the subscriber already has a session available in Interface 1.

  Workaround: There is no workaround.

- CSCue05492

  Symptoms: The DHCP snooping client ignores the IPC flow control events from CF.

  Conditions: This symptom is observed when CF gives flow control off event and the DHCP snooping client does not handle it.

  Workaround: There is no workaround.

- CSCue15619

  Symptoms: The SBC CLI hangs after configuring signaling-peer-port.

  Conditions: This symptom is observed after you re-configure the signaling-peer-port when the adj is already attached, the new vty terminal would be hung.

  Workaround: Perform “no attach” adjacency first.

- CSCue17116

  Symptoms: The following error message is logged during churning of EoGRE GTP sessions.

  ```
  Traceback %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!)
  ```

  Conditions: This traceback is logged while churning 18,000 EoGRE GTP sessions.

  Workaround: There is no workaround.

- CSCue17123

  Symptoms: The ATM/IMA ping fails from 2nd interface post SSO in Cisco IOS XE 3.9 Release.

  Conditions: This symptom is observed when you have multiple ATM interfaces and issue switchover. Traffic does not flow from 2nd interface after switchover.

  Workaround: There is no workaround.

- CSCue18133

  Symptoms: The Cisco 7600 Router crashes at show_li_users.

  Conditions: This symptom is observed under the following conditions:

  1. In li-view, create an username: lawful-intercept and li_user password: lab1.
  2. Then, attempt its delete by “no username li_user”.
  3. Later, show users of LI.

  Workaround: There is no workaround.

- CSCue25575

  Symptoms: The crash is observed for SDP pass through or call forward or antitrombone cases.

  Conditions: The crash is observed for a basic call involving SDP pass through or call forward or antitrombone cases.

  Workaround: There no workaround.

- CSCue27652

  Symptoms: The ATM interfaces are getting deleted on SSO.

Conditions: This symptom is observed when the ATM Interfaces are deleted on standby after IM OIR.

Workaround: There is no workaround.

- CSCue27698

  Symptoms: Configuring long list of REP block port preferred VLAN will result in losing part of this configuration after the reload.

  Example: Configuration like this

  ```
  rep block port preferred vlan
  76-86,94,98,200-201,400,592-593,606-607,611,633,635-636,638,640,643,901-902,1026,
  1539,2007-2064
  ```

  will result in two lines in running configuration:

  ```
  rep block port preferred vlan 76-86,94,98,200-201,400,592-593,606-607,611,633
  rep block port preferred vlan 635-636,638,640,643,901-902,1026,1539,2007-2064
  ```

  after the reload second line will overwrite the first and only one line will remain:

  ```
  rep block port preferred vlan 635-636,638,640,643,901-902,1026,1539,2007-2064
  ```

  Conditions: This symptom is observed after the reload.

  Workaround: Reconfigure the REP block list after the reload.

- CSCue30237

  Symptoms: The CFM trace route fails.

  Conditions: This symptom occurs in CFM with VPLS in the core. Configure the Up MEP on BD which has the VFI terminated.

  Workaround: There is no workaround. The issue is specific to VPLS in the core and Up MEP on the same BD.

- CSCue30590

  Symptoms: Packet loss are seen over pseudowire and high CPU.

  Conditions: This symptom is observed when IPv6 site-local multicast MAC traffic is sent over SVI EoMPLS, the traffic is looped between the PE of the EoMPLS.

  Workaround: There is no workaround.

- CSCue31321

  Symptoms: A Cisco router or switch may unexpectedly reload due to bus error or SegV when running the **how ip cef ... detail** command.

  Conditions: This symptom is observed when the output becomes paginated (---More---) and the state of the CEF adjacency changes while the prompt is waiting on the more prompt.

  Workaround: Set “term len 0” before running the **how ip cef ... detail** command.

- CSCue38489

  Symptoms: Multicast packets (both data and control) get duplicated when they egress out of the port channel with ten gigabit interface members.

  Conditions: This symptom occurs when we create the below configurations. Duplicate packets with Service Instance/ EFPs for multicast packets arise when the below conditions are true:

  – The port channel has only ten gigabit interfaces as members.

  – Multicast, unlearnt unicast, or broadcast packets egress out on the port channel interface.

But after reloading the box with the given configurations, the problem is seen only when admin shut/no shut is performed at least once on the port channel interface.

Workaround: There is no workaround.

- CSCue40354

  Symptoms: CPUHOG error message is seen at nile_mgr_bdomain_get_efp_count and then followed by a crash.

  Conditions: This symptom is observed on booting the router with scaled mVPN configurations.

  Workaround: There is no workaround.

- CSCue43250

  Symptoms: IMA configuration will not be parsed correctly after the router reload, when the A903-IM40S is inserted in Bay4/Bay5 of the ASR903 router.

  Conditions: This symptom is observed when the IMA and ATM interfaces are adjacent. This happens only for IM inserted on Bay 4 or above.

  Workaround: Insert the IM in bay 0 bay 3 if you want the IMA and ATM parsing to work, or reconfigure the ATM and IMA interfaces, for it to work.

- CSCue43776

  Symptoms: Cisco IOS memory leak at com.cisco.cxsc-cxsc-5651.

  Conditions: This symptom is observed when K2 firewall and kWAAS are configured.

  Workaround: There is no workaround.

- CSCue45934

  Symptoms: This problem is specific to the Catalyst 6000 platform. With IPv4 crypto map, ICMP echo reply is not triggered from the remote end.

  Conditions: This symptom is observed in IPv4 crypto map configuration and Catalyst 6000 platform.

  Workaround: There is no workaround.

- CSCue46685

  Symptoms: Client MAC/framed IP missing in the coa:session query response from ISG.

  Conditions: The symptom is observed when you do a COA account-query for lite-session.

  Workaround: There is no workaround.

- CSCue52708

  Symptoms: The router crashes upon defaulting the backup switch interface configuration immediately after doing shut/no shut on it.

  Conditions: This symptom is observed after the admin shut/no shut wait for some time (till the port comes up) before defaulting the interface configuration.

  Workaround: There is no workaround.

- CSCue55739

  Symptoms: PfR MC/BR session may be flapped, if PfR learn is configured with scale configuration.

  Conditions: This symptom may be observed, if PfR traffic-classes are learned by PfR global **learn** configuration.

  Workaround: Disable PfR global **learn** by configuring **traffic-class filter access-list** pointing to the **deny ip ip any** ACL, and configure PfR learn “list”.

- CSCue59773

  Symptoms: ARP for default gateway will not be resolved

  Conditions: This symptom is observed when client has a lite session in ISG and he clears his ARP table and then tries to query for the ARP second time

  Workaround: Do not clear the ARP entry in the client.

- CSCue65523

  Symptoms: The **archive download** command fails in mcp_dev/xe39 nightly image which is being used for software up-gradation.

  Conditions: This symptom is observed only on the whales 2 box.

  Workaround: There is no workaround.

- CSCue67751

  Symptoms: The classification based on QoS group egress policy is not working correctly.

  Conditions: With L3VPN configuration, the core interface packets should be classified based on EXP and marked with QoS-group. On the egress interface packets should be classified based on QoS group on the service instance.

  Workaround: There is no workaround.

- CSCue69527

  Symptoms: More than 95 SCCP controlled FXS ports cannot be configured on the Cisco VG350.

  The debug output for “debug ccm-manager config-download errors” is as follows:

  ```
  cmapp_sccp_gw_start_element_handler: warning - max number of interfaces reached.
  ```

  Conditions: This symptom occurs when configuring more than 95 SCCP FXS ports on the Cisco VG350 using CUCM.

  Workaround: There is no workaround.

- CSCue76251

  Symptoms: A BFD session is created for tunnel-tp without any BFD configuration underneath it.

  Conditions: This symptom occurs only on bootup and when there is no BFD configuration underneath tunnel-tp.

  Workaround: There is no workaround.

- CSCue77909

  Symptoms: The interface link shows UP, without fiber IN.

  Conditions: This symptom is observed with OCP vendor 100FX SFP on whales2.

  Workaround: There is no workaround.

- CSCue85737

  Symptoms: ASR with PKI certificate may crash when issuing **show crypto pki certificate** command.

  Conditions: This symptom is observed when the **show crypto pki certificate** command is issued on ASR with PKI certificate.

  Workaround: There is no workaround.

- CSCue86147

  *Policy with class map match-all with prec 1 and 2 is accepted for WRED.

- CSCue86845

  Symptoms: An unexpected behavior caused with Ingress QoS, caused by commit CSCuc01040.

  Conditions: This symptom is observed with Ingress QoS, caused by commit CSCuc01040.

  Workaround: There is no workaround.

- CSCue89385

  Symptoms: Traffic from routed VPLS does not trigger ARP.

  Conditions: This symptom is observed in a routed VPLS network that has multiple CE routers connected to the PE router. The issue occurs when a local CE router is connected to the PE router via an EVC and when a ping is sent from a local CE router to the remote CE router.

  Workaround: Ping the first interface VLAN of the EVC to resolve the ARP.

- CSCue92705

  Symptoms: The “DHCPD Receive”, “CDP Protocol”, and “Net Background” processes leaks could be seen after disabling “macro auto monitor”.

  Conditions: This symptom is observed in Cisco IOS 15.0(2)SE1 Release, 2960S, dhcp, cdp traffic, and link flapping.

  Workaround: Configure “no service dhcp” if the switch is not a DHCP server.

  ```
  Configure device-sensor filter-spec cdp exclude all device-sensor filter-spec dhcp
  exclude all device-sensor filter-spec lldp exclude all
  ```

- CSCue97986

  Symptoms: Calls hang at SIP, CCAPI and VOIP RTP components (but are cleared in the dataplane of the Cisco ASR 1000 series platform).

  Conditions: This symptom occurs when a video call is setup as an audio call. The call then gets transferred with REFER but the caller hangs up the call before the call gets transferred. This is an intermittent problem.

  Workaround: If there is an SIP call dangling (sh sip call sum), then use the **clear cal voice causecode 16** command to clear the dangling call.

- CSCuf16504

  Symptoms: Classification based on the QoS group along with prec/dscp at the egress policy does not function as expected.

  Conditions: This symptom occurs with L2VPN/L3VPN configuration. On the core interface, packets should be classified based on exp and marked with the QoS group. On the egress interface, packets should be classified based on the QoS group and prec/dscp/cos inner.

  Workaround: There is no workaround.

- CSCuf17009

  Symptoms: With PIM enabled on a P2P GRE tunnel or IPSec tunnel, the SP of the Cisco 7600 series router might crash.

  Conditions: This symptom occurs when there are more number of tunnels going via the same physical interface. This issue is seen in Cisco IOS SREx and Cisco IOS 15.S based releases only.

  Workaround: There is no workaround.

- CSCuf20407

  Symptoms: Tracebacks are seen on Whales2 bootup.

Conditions: This symptom occurs when Whales2 boots with Cisco IOS Release 15.2(4)S0.2, Cisco IOS Release 15.3(1)S0.1 or prior releases on the new Rev 2 HW.

Workaround: There is no workaround.

- CSCuf20537

  Symptoms: The router crashes due to null pointer dereference.

  Conditions: This symptom occurs with the C4 VSS system (2 sup vss) with dual-homed fex stack (This has not been seen on other platforms, but the fix is ported as a precautionary measure). During the first SSO, no crash is observed [Active and Standby (Hot-Standby)]. During the second SSO, a is crash observed.

  Workaround: There is no workaround.

- CSCuf25555

  Symptoms: Policy-based routing stops working after the router reloads.

  Conditions: This symptom occurs when multiple next-hops configured on the same route map are reachable through the same interface.

  Workaround: Remove and reconfigure the route-map.

  Further Problem Description: This is a specific scenario where multiple next-hops configured on the same route map are reachable through the same physical interface on different VLANs.

  After reload, when the physical interface comes up, adjacency for all configured next-hops on different sequence numbers of the same route map were notified to the PD client simultaneously.

- CSCuf30554

  Symptoms: A traffic drop is seen with scalable EoMPLS VCs going over TE tunnels. The issue is reproduced if a large or small number of tunnels are present and they undergo a lot of flap events.

  Conditions: This symptom occurs when the MPLS label for a TE internal label gets allocated with a value having more than 20 bit.

  Workaround: There is no workaround.

- CSCuf43548

  Symptoms: When the POS Rx fiber at the tail end of the MPLS TE FRR is pulled, the FRR takes longer than 200ms to cut over to the other tunnel.

  Conditions: This symptom occurs with POS MPLS TE FRR when the head end receives a remote defect due to the Rx fiber pull at the tail end. Remote defects do not trigger FRR quickly.

  Workaround: There is no workaround.

- CSCuf65255

  Symptoms: CPU hog is caused by unnecessary calling of avl_get_next to calculate the dynamic MPLS label range for each of the service instances configured (especially for L3VPN services).

  Conditions: This symptom occurs under the following conditions:

  1. When running configuration is accessed using the “show running-config” CLI.
  2. While copying running configuration to either the startup configuration or the local disk or the tftp server.

  This results in the copy operation taking more than 300 seconds (for an average configuration size of 1000kB).

  Workaround: Reducing the number of BGP routes injected for L3VPN sessions causes the CPU hog to last for a smaller duration.

- CSCug31561

  A vulnerability in the DHCP implementation of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  The vulnerability occurs during the parsing of crafted DHCP packets. An attacker could exploit this vulnerability by sending crafted DHCP packets to an affected device that has the DHCP server or DHCP relay feature enabled. An exploit could allow the attacker to cause a reload of an affected device.

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

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-dhcp

  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight 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 September 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_sep13.html

Open Caveats—Cisco IOS Release 15.2(4)S2

Cisco IOS Release 15.2(4)S2 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveat in this section is open in Cisco IOS Release 15.2(4)S2. This section describes only select open caveats.

- CSCud36113

  Symptoms: Ping fails between CE routers.

  Conditions: This symptom is observed when you configure MPLS VPN Inter-AS IPv4 BGP Label Distribution and flaps "mpls bgp forwarding" in the interface between ASBRs.

  Workaround: Removing and adding (flapping) the static routes between ASBRs resolves the issue.

Resolved Caveats—Cisco IOS Release 15.2(4)S2

Cisco IOS Release 15.2(4)S2 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveats in this section are resolved in Cisco IOS Release 15.2(4)S2 but may be open in previous Cisco IOS releases.

- CSCtg39957

  The Resource Reservation Protocol (RSVP) feature in Cisco IOS Software and Cisco IOS XE Software contains a DoS vulnerability.

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

  This advisory is available at the following link:

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

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

- 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

- CSCtk15666

  Symptoms: The Cisco IOS password length is limited to 25 characters.

  Conditions: This symptom is observed on Cisco NG3K products.

  Workaround: There is no workaround.

  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

- CSCts52120

  Symptoms: Tracebacks are seen for PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT.

  Conditions: This symptom is observed with RPSO.

  Workaround: There is no workaround.

- CSCts75737

  Symptoms: Tracebacks are seen at swidb_if_index_link_identity on the standby RP.

  Conditions: This symptom is observed when unconfiguring and reconfiguring "ipv4 proxy-etr" under the router LISP.

Workaround: There is no workaround.

- CSCtu28696

  Symptoms: A Cisco ASR 1000 crashes with **clear ip route ***.

  Conditions: This symptom is observed when you configure 500 6RD tunnels and RIP, start traffic and then stop, and then clear the configuration.

  Workaround: There is no workaround.

- CSCtw65575

  Symptoms: The router may unexpectedly reload when OSPFv3 MIB is polled via SNMP.

  Conditions: This symptom occurs when OSPFv3 is configured with area ranges whose prefix length is /128. A router with no area ranges is not vulnerable.

  Workaround: Configure area ranges to have a smaller prefix length (that is, in the range of /0 to /127).

- CSCtw80678

  Symptoms: Multilink PPP ping fails when the serial interfaces experience QMOVESTUCK error.

  Conditions: This symptom may be observed if multilink PPP member links and serial interfaces on which the QMOVESTUCK error is reported are on the same SPA.

  Workaround: “no shut” the interface with the QMOVESTUCK error message, remove QoS policies on the interface and subinterfaces, and remove the interface from the T1/T3 controller. Then, rebuild the configuration.

- CSCtx31177

  Symptoms: RP crash is observed on avl_search in a high scaled scenario.

  Conditions: This symptom is observed in a high scaled scenario with continuous traffic flow.

  Workaround: There is no workaround.

- CSCtx34823

  Symptoms: OSPF keeps on bringing up the dialer interface after idle-timeout expiry.

  Conditions: This symptom occurs when OSPF on-demand is configured under the dialer interface.

  Workaround: There is no workaround.

- CSCty44654

  Symptoms: The router crashes when trying to test the MVPN6 functionality.

  Conditions: This symptom is observed with the following conditions:

  - Configure the router to test the MVPN6 functionality.
  - Delete the VRF associated with the interface in the MVPN6 test configuration.

  Workaround: There is no workaround.

- CSCty57476

  Symptoms: The BGP GSHUT feature needs to add support for the AA:NN format for community.

  Conditions: This symptom is observed when support is added for the AA:NN format for community when using the BGP GSHUT feature.

  Workaround: The <1-4294967295> community number can be used instead of the AA:NN format.

- CSCty73682

  Symptoms: A small percentage of IPv6 packets that should be blocked by an interface ACL is instead pass through.

  Conditions: This symptom occurs in certain conditions, when an IPv6 ACL is applied to an interface, a small percentage of IPv6 packets that would otherwise be dropped, will instead bypass an ACL and get through.

  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 5/4.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:U/RC:C

  CVE ID CVE-2012-3946 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

- CSCty74859

  Symptoms: Memory leaks on the active RP and while the standby RP is coming up.

  Conditions: This symptom is observed when ISG sessions are coming up on an HA setup.

  Workaround: There is no workaround.

- CSCtz26682

  Symptoms: Switchover/reload fails in the Cisco ASR 903 HA setup due to the "LICENSE-3-ISSU_ERR: ISSU start nego session FAILED, error:-287" error message.

  Conditions: This symptom is observed with the Cisco ASR 903 router. This issue is seen only when doing a Route Processor (RP) switchover using the **redundancy force-switchover** command.

  Workaround: There is no workaround.

- CSCtz28023

  Symptoms: Traffic is not forwarded for a few mroutes.

  Conditions: This symptom is observed when multiple routers in the network are reloaded simultaneously.

  Workaround: Using the **clear ip mroute vrf** *vrf name* command may resolve the issue.

- CSCtz34869

  Symptoms: Aps-channel stops working.

  Conditions: This symptom occurs with an open ring and is seen in the following scenario:

  ```
  A1(po2)(RPL)<======>(po2)A3  (gig3/2)<=======>(gig3/3)A4
  ```

  Shut down gig3/2 on A3 does not make A1 into protection.

  - Debugs show no SF packets are being transmitted to A1 which is connected to A3 via "Port-channel".
  - A1 (po2) is RPL of the ring. It is not going to be unblocked even after the A3-A4 link goes down.

  Workaround: Reload the line card.

- CSCtz50683

  Symptoms: Upon removing 10 x MDLP sessions, one or more hardware adj remains. This happens due to incorrect removal of LSPs.

  Conditions: This symptom is observed when more than eight sub-LSPs occur.

  Workaround: Use no more than eight sub-LSPs.

- CSCtz55979

  Symptoms: The router crashes.

  Conditions: This symptom occurs when you configure CFM, SCE over MPLS, VPLS, or G.8032 services while running SNMP polling.

  Workaround: There is no workaround.

- CSCtz58189

  Symptoms: The router crashes on using the **config replace** command with certain QoS configured on the box.

  Conditions: This symptom occurs when certain QoS are configured on the box are replaced with the configuration that is removing the configurations.

  Workaround: There is no workaround.

- CSCtz58391

  Symptoms: Ingress QoS Tcams are not cleared after certain dynamic changes.

  Conditions: This symptom is observed on removing the encapsulation from the service instance and then deleting the service instance. QoS Tcams are not cleared.

  Workaround: Instead of deleting the encapsulation first, delete the service instance first.

- CSCtz88879

  Symptoms: When testing for DMVPN in a HUB-SPOKE topology, where there are 170 tunnels protected with IPsec on Spoke and one mGRE tunnel on hub. B2B redundancy is configured. No QoS is applied on the scaled IPsec tunnels. Upon doing SSO with this configuration, the "%VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnelx: allocated idb has invalid vlan id" error message is seen repeatedly on the new active and the router becomes almost inaccessible. As can be seen from the **show vlan int usage** command output, there are more than 3K free VLANs on both the hub and spoke.

  ```
  *May 14 12:31:10.315: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel87: allocated idb has
  invalid vlan id
  *May 14 12:31:10.511: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel26: allocated idb has
  invalid vlan id
  *May 14 12:31:10.543: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel28: allocated idb has
  invalid vlan id
  *May 14 12:31:10.575: %VPNSMIOS-3-MACEDONTUNNELVLANERR: Tunnel90: allocated idb has
  invalid vlan id
  ```

  After a continuous flood of error messages, a Granikos crash is seen, and the **show cry eli** command shows only one SPA and this SPA is stuck in INIT state.

  Conditions: This symptom occurs when doing a shut/no shut using the **interface range** command, and once all tunnels are up, doing an SSO.

  Workaround: There is no workaround.

- CSCua01641

  Symptoms: The router's NAS-IP address contained in the RADIUS accounting-on packet is 0.0.0.0:

RADIUS: Acct-Session-Id [44] 10 "00000001" RADIUS: Acct-Status-Type [40] 6 Accounting-On [7] RADIUS: NAS-IP-Address [4] 6 0.0.0.0

RADIUS: Acct-Delay-Time [41] 6 0

Conditions: This symptom occurs when you restart the router.

Workaround: There is no workaround.

- CSCua12396

  Symptoms: IPv6 multicast routing is broken when there are master switchover scenarios with a large number of members in stack. This issue is seen on platforms such as Cisco 3750E and Cisco 3750X where IPV6 multicast routing is supported.

  Conditions: This symptom is observed when IPV6 multicast routing is configured, mcast routes are populated, and traffic is being forwarded. In case of master switchover, synchronization between the master and members is disrupted. This issue is seen only for IPv6 multicast routing. This issue has been observed with a 9-member stack and either during the first or second master switchover. No issues are seen for IPv4 multicast routing.

  Workaround: This scenario was tested with a 5-member stack, and no issues were seen. It is recommended to enable IPv6 multicast routing when there is deployment with low members in a stack.

- CSCua15003

  Symptoms: When a call is canceled mid-call, the CUBE may not release the transcoder resource for the call. As a result, there is a DSP resource leak.

  Conditions: This symptom can occur in the following situations:

  – CUBE receives 180 ringing with an SDP session.

  – “media transcoder high-density” is enabled.

  Workaround: Disable “media transcoder high-density”.

- CSCua20373

  Symptoms: After SSO, all the GRE tunnels get admin down and stay down until the security module SSC-600/WS-IPSEC-3 comes up. Complete traffic loss is seen during this time.

  Conditions: This symptom is observed when Vanilla GRE tunnels are configured in the system where HA and the IPsec Module SSC-600/WS-IPSEC-3 card is present, “crypto engine mode vrf” is configured, and SSO is issued.

  Workaround: Remove the “cryto engine mode vrf” configuration if IPsec is not enabled on the router.

- CSCua24689

  Symptoms: Fragments are sent without label resulting in packet drops on the other side.

  Conditions: This symptom is observed with the following conditions:

  – MPLS enabled DMVPN tunnel on egress.

  – VFR on ingress.

  Workaround: Disable VFR, if possible.

- CSCua26064

  Symptoms: IPv6 routes in the global routing table take up different adjacency entries.

Conditions: This symptom is observed when there are four core facing tunnels that load balance traffic to these prefixes. The **show mls cef ipv6** *prefix* **detail** command shows the different adjacencies taken by different prefixes.

Workaround: Have a single tunnel on the core facing side, instead of a load balanced path.

- CSCua31934

  Symptoms: A crash is seen at __be_address_is_unspecified.

  Conditions: This symptom is observed with the following conditions:

  1. It occurs one out of three times and it is a timing issue.
  2. DMVPN tunnel setup between Cisco 2901 as the spoke and Cisco ASR 1000 as the hub.
  3. Pass IPv4 and IPv6 traffic between the hub and the spoke for 5-10 minutes.
  4. It can occur with v6 traffic alone.
  5. If you remove the tunnel interface on the Cisco ASR and add it again using **conf replace nvram:startup-config** command, the crash will occur.

  Workaround: Use CLI to change configuration instead of the rollback feature.

- CSCua39390

  Symptoms: The PRI configuration (voice port) is removed after a reload.

```
interface Serial1/0:23          ^
% Invalid input detected at '^' marker.
no ip address
% Incomplete command.
encapsulation hdlc
   ^
% Invalid input detected at '^' marker.
isdn incoming-voice voice
       ^
% Invalid input detected at '^' marker.
no cdp enable
        ^
% Invalid input detected at '^' marker.
voice-port 1/0:23
           ^
% Invalid input detected at '^' marker.
Also getting trace back
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F0478z 0x607F72C0z 0x60722F38z 0x6070A300z
0x6070A9CCz 0x603E1680z 0x6029541Cz 0x60298F6Cz 0x6029AD48z 0x6029D384z
0x6062BC68z 0x60632424z 0x60635764z 0x60635CE0z 0x60877F2Cz
%SYS-2-INTSCHED: 'may_suspend' at level 3  -Process= "Init", ipl= 3, pid= 3
-Traceback= 0x607EE41Cz 0x630F04E4z 0x607F7154z
```

  Conditions: This symptom is observed with Cisco IOS Release 15.1(3)T and Cisco IOS Release 15.1(4)M4. This issue is not seen with Cisco IOS Release 12.4(24)T6 or earlier release. The issue occurs after reload.

  Workaround: Reapply the configuration after the router comes back up.

- CSCua41333

  Symptoms: A crash occurs at __be_ipsub_dp_disconnect_session with DHCP scale when routed/L2-connected sessions are brought up/down one after the other.

  Conditions: This symptom occurs when you bring up scale routed DHCP sessions, later bring them down, and then bring up scale L2-connected DHCP sessions on the same interface or vice versa.

Workaround: Reload the router after changing the configuration.

- CSCua42523

  Symptoms: The router crashes and reloads when “options-keepalive” is enabled on a dial peer which has session target as sip-server.

  Conditions: This symptom is observed when enabling “options-keepalive” which has a session target as sip-server. Also, “sip-server” is configured under “sip-ua” and has a DNS address which resolves to an IPv6 address.

  Workaround: Do not enable “options-keepalive” for dial peer.

- CSCua45206

  Symptoms: The hub router crashes while removing the Stale Cache entry.

  Conditions: This symptom occurs when two spokes are translated to the same NAT address.

  Workaround: Spokes behind the same NAT box must be translated to different post-NAT Addresses.

- CSCua49764

  Symptoms: The WAAS-Express device goes offline on WCM.

  Conditions: This symptom occurs when a certificate is generated using HTTPS when using the Cisco IOS Release 15.1(3)T image. Once upgraded to Cisco IOS Release 15.2(3)T, the WAAS-Express device goes offline on WCM.

  Workaround: Configure an rsakeypair on the TP-self-signed trustpoint with the same name and execute the **enroll** command again or delete the self-signed trustpoint point and reenable the HTTP secure-server.

- CSCua55785

  Symptoms: Build breakage occurs due to the fix of CSCtx34823.

  Conditions: This symptom occurs with the CSCtx34823 fix.

  Workaround: CSCtx34823 change may be unpatched from the code-base.

- CSCua56999

  Symptoms: Abnormal line card reload occurs.

  Conditions: This symptom occurs when an MVPNv6 scaled router acts as PE on which source traffic is ingressing and the line card is connected on the access side.

  Workaround: There is no workaround.

- CSCua61330

  Symptoms: Traffic loss is observed during switchover if,

  1. BGP graceful restart is enabled.
  2. The next-hop is learned by BGP.

  Conditions: This symptom occurs on a Cisco router running Cisco IOS XE Release 3.5S.

  Workaround: There is no workaround.

- CSCua81998

  Symptoms: Doing ISSU RV in a Cisco 7600 box with the ES40 line card may sometimes cause a crash in the ES40 line card.

  Conditions: This symptom is observed with ISSU RV with Cisco IOS XE Release 3.7S, or Cisco IOS XE Release 3.8S to Cisco IOS XE Release 3.6.1S.

Workaround: There is no workaround.

- CSCua82440

  Symptoms: FNF records do not get exported when a user reloads the router.

  Conditions: This symptom occurs if a user configures a nondefault export-protocol, that is, anything other than “netflow-v9”. If the user configures a nondefault export-protocol such as IPFIX or netflow-v5, after saving the configuration to the start-up configuration and reloading the router, the exporter will not export any records.

  Workaround: Either one of the following methods will fix this issue:

  1. Remove and reconfigure the exporter configuration after reload.
  2. Change the export-protocol to the default value (netflow-v9).

- CSCua85239

  Symptoms: Flapping BGP sessions are seen if large BGP update messages are sent out and BGP packets are fragmented because midpoint routers have the smaller "mtu" or "ip mtu" configured.

```
*Jun  3 18:20:20.792 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:30.488 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:36.451 UTC: %BGP-5-ADJCHANGE: neighbor 6.6.6.5 Down BGP
Notification sent
*Jun  3 18:20:36.451 UTC: %BGP-3-NOTIFICATION: sent to neighbor 6.6.6.5 4/0
(hold time expired) 0 bytes
*Jun  3 18:20:36.569 UTC: %BGP_SESSION-5-ADJCHANGE: neighbor 6.6.6.5 VPNv4
Unicast topology base removed from session  BGP Notification sent
*Jun  3 18:20:40.184 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:44.619 UTC: %BGP-5-ADJCHANGE: neighbor 6.6.6.5 Up
*Jun  3 18:20:49.926 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
*Jun  3 18:20:59.604 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179)
to 2.2.2.5(17744) tableid - 0
```

  Conditions: This symptom is observed between two BGP peers with matching MD5 passwords configured and can be triggered by the following conditions:

  - If the midpoint path has the “mtu” or “ip mtu” setting that is smaller than the outgoing interface on BGP routers, it will be force the BGP router to fragment the BGP packet while sending packets through the outgoing interface.
  - Peering down and the MD5 error do not always occur. They occur only once or twice within 10 tests.

  Workaround: There is no workaround.

- CSCua85604

  Symptoms: Ingress Qos on EVC stops working after reload or after interface flap.

  Conditions: This symptom occurs only on EVC QOS.

  Workaround: Remove and reconfigure the QOS on EVC.

- CSCua90061

  Symptoms: The WS-IPSEC-3 Module crashes post configuration change.

  Conditions: This symptom occurs when you dynamically modify the GRE tunnel protected with IPsec to the sVTI tunnel and vice versa while traffic is traversing across the IPsec tunnel.

  Workaround: There is no workaround.

- CSCua91473

  Symptoms: Memory leak occurs during rekey on the IPsec key engine process.

  Conditions: This symptom occurs after rekey, when the IPsec key engine does not release KMI memory, causing the IPsec key engine holding memory to keep increasing.

  Workaround: Clear crypto session for IPsec key engine to release memory.

- CSCua91698

  Symptoms: ephone-type disappears from the running-configuration.

  Conditions: This symptom occurs in SRST mode and after reload.

  Workaround: Reconfigure the ephone-type commands and again save to the startup-configuration.

- CSCua99969

  Symptoms: IPv6 PIM null-register is not sent in the VRF context.

  Conditions: This symptom occurs in the VRF context.

  Workaround: There is no workaround.

- CSCub04112

  Symptoms: The router may lose OSPF routes pointing to the reconfigured OSPF interface.

  Conditions: This symptom occurs after quick removal and adding of the interface IP address by script or copy and paste.

  For example, configure the following:

```
interface Ethernet0/0
 ip address 1.1.100.200 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
end
```

  Then, quickly remove/add the IP address:

```
conf t
interface Ethernet0/0
 no ip address 1.1.100.200 255.255.255.0
 ip address 1.1.100.200 255.255.255.0
 ip ospf network point-to-point
 ip ospf 1 area 0
end
```

  Workaround: Insert a short delay in between commands for removing/adding the IP address. The delay should be longer than the wait interval for LSA origination; by default, it is 500 ms. Or, refresh the routing table by “clear ip route *”.

- CSCub04345

  Symptoms: The Cisco ASR-1002-X freezes after four hours with a scaled “path-jitter” sla probe configuration.

  Conditions: This symptom is observed with a scaled “path-jitter” sla probe configuration.

  Workaround: There is no workaround.

- CSCub04982

  Symptoms: In an IPFRR configuration, a traceback is seen about changing the FRR primary OCE where the new OCE has a different interface and next-hop, which blocks such a linkage.

Conditions: This symptom occurs while changing the FRR primary OCE interface to a new OCE with a different interface.

Workaround: There is no workaround.

- CSCub06859

  Symptoms: OSPFv2 NSR on quad-sup VSS does not work. The router stops sending hello packets after switchover.

  Conditions: This symptom is observed with quad-sup VSS with OSPFv2 NSR.

  Workaround: Clear the IP OSPF process after NSR switchover.

- CSCub07855

  Symptoms: The VRF error message is displayed in the router.

  Conditions: This symptom occurs upon router bootup.

  Workaround: There is no workaround.

- CSCub15105

  Symptoms: Traffic drop of MVPNv6 data MDT packets is seen.

  Conditions: This symptom is observed on doing a VRF delete and adding it on the encapsulated PE in a scaled MVPNv6 setup; the L3 DENY RESULT drop counters increment for the encapsulated VLAN v4. From a multicast point of view, the drop is at the point where the packet reaches the encapsulated VLAN v4 to proceed further with backbone forwarding.

  Workaround: There is no workaround.

- CSCub15402

  Symptoms: A VRF cannot be deleted. The following error message is displayed:

  ```
  error message "% Deletion of VRF VPNA in progress; wait for it to complete".
  ```

  Conditions: This symptom occurs after having previously issued “sh ip cef vrf * sum”.

  Workaround: There is no workaround. Reboot is required to remove the VRF.

- CSCub22049

  Symptoms: Native MCAST traffic is not forwarded over a nile1 after core interface shut/no shut.

  Conditions: This symptom is observed after doing shut/no shut or interface flap a couple of times.

  Workaround: “clear ip mroute <mcast_group>” or “clear ip route *”.

  Further Problem Description: Not all the multicast groups will be affected. The behavior is inconsistent.

- CSCub23231

  Symptoms: Very specific events/packet types cause the ES20 LC to stop passing traffic. Information on these events and packets that lead to the issue are not known currently.

  Conditions: This symptom occurs when the ES20 interface has an EVC or MPLS configuration.

  Workaround: Reload LC.

- CSCub31477

  Symptoms: A Cisco ISG router configured for Layer 2 Connected Subscriber Sessions does not respond to ARP replies once a subscriber ARP cache has expired.

Conditions: This symptom occurs when the router is configured as ISG L2-Connect, the router has configured HSRP as the high-availability method, and the subscriber-facing interface is configured with “no ip proxy arp”. This issue is not seen if either HSRP is removed or if “ip proxy arp” is enabled.

Workaround: Clear the subscriber session. After the subscriber is reintroduced, the issue is resolved. You can also configure “ip proxy arp” on the HSRP-configured interface.

- CSCub33470

  Symptoms: Default profiles showing up as custom.

  Conditions: This symptom is observed with a Cisco Catalyst 3000/Catalyst 4000 platform which supports the IP SLA video operation. This issue has no affect on the operation itself.

  Workaround: There is no workaround.

- CSCub34595

  Symptoms: Enabling Dynamic ARP Resolution (DAI) on a VLAN may cause ARP resolution to fail for hosts in other VLANs.

  Conditions: This symptom is seen when enabling DAI on a VLAN.

  Workaround 1: Enable DAI for the failing VLAN using the **ip arp inspection vlan x** command.

  For example:

```
ip arp inspection vlan 30
 int gi 0/10
  ip arp inspection trust
 int gi 0/11
  ip arp inspection trust
```

  Workaround 2: Enable DAI for the failing VLAN using the **ip arp inspection vlan x** command. Configure an ARP ACL to permit traffic for a valid IP source + MAC source pair using the **arp access- list** *acl_name* command. Configure the DAI filter and associate with the ARP ACL using the **ip arp inspection filter** *acl_name* **vlan x** command. Configure the DAI trust on the egress port using the **ip arp inspection trust**.

  For example:

```
ip arp inspection vlan 20
        arp access-list testacl
            permit ip 10.1.1.3 255.255.255.0 mac 01:00:00:0E:0E:0F
        ip arp inspection filter testacl vlan  20
        int gig0/10
            ip arp inspection trust
```

- CSCub34756

  Symptoms: RP crash is observed at rrr_lm_resource_link_ready after performing SSO on the midpoint router on protect LSP.

  Conditions: This symptom is observed when an RP card hosting the TP tunnel midpoint is undergoing the SSO operation. During SSO recovery, the TP fails to recover the TP tunnel midpoint interface (virtual) that is causing it to send a NULL interface to TE for checking its readiness. TE is not checking the NULL pointer condition and accessing the link elements that are causing the crash.

  Workaround: There is no workaround.

- CSCub36356

  Symptoms: Scaling up routes result in huge memory allocations, eventually depleting the SP memory, leading to MALLOC FAIL and subsequent system crash.

Conditions: This symptom occurs in normal conditions.

Workaround: There is no workaround.

- CSCub38559

  Symptoms: When static recursive routes are used in an MVPNv6 environment, multicast traffic loss can occur due to failure to determine the correct RPF interface for a multicast source or rendezvous point.

  Conditions: This symptom occurs if a static route to an IPv6 address at a remote site (remote side of a VPN cloud) resolves via a BGP route, resulting in a failure to install the required MDT alternate next-hop in the recursively referenced BGP route.

  Workaround: Executing “show ipv6 rpf vrf X <address>” for any address within the recursively referenced BGP prefix range will cause installation of the required alternate next-hop.

- CSCub39296

  Symptoms: Unexpected exception to CPU: vector 200, PC = 0x0. Traceback decode is irrelevant.

  Conditions: This symptom is observed on the ES+ series linecards on a Cisco 7600 series router. Symptom is reported on the ES+ console and in the crashinfo file on the ES+ flash disk. It is not reported in the syslog.

  Workaround: There is no workaround.

- CSCub45809

  Symptoms: Cisco IOS configured for Voice over IP may experience stack corruption due to multiple media loops.

  Conditions: This symptom is observed with a special configuration of IP features, along with disabling the recommended **media flow-around** command. This issue is seen with Cisco IOS Release 15.2(2)T.

  Workaround: Apply the **media flow-around** command.

  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 5.4/4.4:
  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:U/RL:W/RC:C

  CVE ID CVE-2012-5044 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

- CSCub48120

  Symptoms: SP crash is observed at oce_to_sw_obj_type on a router reload.

  Conditions: This symptom is seen with a core link flap at the remote end during IP- FRR cutover.

  Workaround: There is no workaround.

- CSCub49985

  Symptoms: MPLS pseudowire ping from the peer to the Cisco ASR 903 fails if the peer is using TTL-based ping.

  Conditions: This symptom occurs when the peer is using TTL-based ping.

  Workaround: There is no workaround.

- CSCub53398

  Symptoms: The router crashes on bootup.

Conditions: This symptom occurs when the router is booted up with a scaled MVPNv6 configuration. This issue is highly dependent on the “back walk” timing and sequence; hence, the probability to encounter the issue is low.

Workaround: Disable power to all DFC modules on reload and bring them up one by one post reload.

- CSCub54261

  Symptoms: In an MLDP + MVPNv6 setup, abnormal RP reload occurs after the deletion and addition of few subinterfaces on the encapsulated PE.

  Conditions: This symptom occurs after deletion and addition of few subinterfaces on the router acting as the encapsulated PE on the access side for a few VRFs running MLCP inband.

  Workaround: There is no workaround.

- CSCub58312

  Symptoms: When IGMP query with source IP address 0.0.0.0 is received on an interface, it is marked as mrouter port for that VLAN.

```
Router#show ip igmp int vlan 1
Vlan1 is up, line protocol is up
  IGMP querying router is 0.0.0.0 <----

Router#sh ip igmp snooping mrouter
vlan            ports
-----+---------------------------------------
   1  Po1,Po8,Router<-----
```

  Conditions: This symptom is observed when IGMP query with source IP address 0.0.0.0 is received.

  Workaround: There is no workaround.

- CSCub68933

  Symptoms: Incorrect MAC learning is observed over pseudowires that are part of HVPLS, causing traffic failure.

  Conditions: This symptom is observed when VPLS autodiscovery is in use, with MPLS over SVI in the core. This issue is also seen with LDP-based VPLS, when split horizon-enabled pseudowires are configured after the non-split horizon-enabled pseudowires.

  Workaround: There is no workaround.

- CSCub70336

  Symptoms: The router can crash when “clear ip bgp *” is done in a large-scale scenario.

  Conditions: This symptom is observed only in a large-scale scenario, with tens of thousands of peers and several VPNv4/v6 prefixes.

  Workaround: “clear ip bgp *” is not a very common operation. Hence, this issue has not been observed by customers. The crash can only happen when “clear ip bgp *” is done. The workaround is not to execute “clear ip bgp *”.

- CSCub73177

  Symptoms: RP crash occurs.

  Conditions: This symptom occurs upon router reload

  Workaround: There is no workaround.

- CSCub73787

  Symptoms: The RSP720 may crash if a high rate of traffic is punted to the RP.

Conditions: This symptom occurs on a Cisco 7600 with RSP720. It is specific to a driver used only by the RSP720. Other supervisor models are not affected. The issue is only seen in Cisco IOS Release 15.1(03)S and later releases, because of a code change made to the RSP720 driver.

Workaround: Isolate and stop the traffic being punted to the RP.

- CSCub79035

  Symptoms: Multicast traffic will get route cached on the receiver/decap node resulting in traffic drop and slight increase in RP/SP CPU.

  Conditions: This symptom is seen when multicast traffic flowing over GRE tunnel protected with IPsec and PIM is enabled on the GRE tunnel.

  Workaround: There is no workaround.

- CSCub79590

  Symptoms: The **match user-group** commands do not appear in the running configuration after being configured.

  Configure an inspection type class-map:

```
class-map type inspect TEST
    match protocol tcp
    match user-group cisco
```

  Save the configuration. Try to view the configuration in the running configuration:

```
hostname# show run class-map
building configuration...

Current configuration : 66 bytes
!
class-map type inspect match-all TEST
   match protocol tcp
end
```

  But, view the configuration directly in the class-map:

```
hostname# show class-map type inspect
   Class Map type inspect match-all TEST (id 1)
     Match protocol tcp
     Match user-group cisco
```

  The configuration never shows up in the running configuration, but it is in the class-map configuration. As a note, the functionality exists on the ZBFW, but the configuration does not show up in the running configuration.

  Conditions: This symptom is only observed with the **match user-group** commands.

  Workaround: This issue only affects devices after a reload as the router will read the startup configuration, which will not have the **match user-group** command. As a result, the **match user-group** commands need to be reentered after ever reload.

- CSCub80386

  Symptoms: The following interface configuration should be used:

```
interface Ethernet2/1
description lanethernet1
ipv6 enable
ospfv3 100 network manet
ospfv3 100 ipv6 area 0
```

Dead interval is calculated according to network type; in this case, it is 120s. Issue the **no ospfv3 dead-interval**command on dead interval. Dead interval is set to the default of 40s instead of 120s, which is correct for manet or P2MP interface types.

Conditions: This symptom is an OSPFv3-specific issue (see the configuration example).

Workaround: Configure dead interval explicitly or reapply the network command.

- CSCub80710

  Symptoms: SSL handshake between Cisco VCS and the Cisco ASR fails if the Cisco ASR is running Cisco IOS XE Release 3.7S.

  Conditions: This symptom occurs in a working setup, if the Cisco ASR is upgraded to Cisco IOS XE Release 3.7S, then SSL handshake and subsequently SIP-TLS calls start to fail. If in the same setup, the Cisco ASR is downgraded back to Cisco IOS XE Release 3.5S or Cisco IOS XE Release 3.4.4S, then the calls work (without requiring any additional changes).

  Workaround: There is no workaround.

- CSCub82471

  Symptoms: BFD session flapping occurs or fails to get established on flapping REP ring.

  Conditions: This symptom is observed with the software BFD session or echo mode.

  Workaround: Disable echo mode.

- CSCub86706

  Symptoms: After multiple RP switchover, the router crashes with the “UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP HA SSO” error.

  Conditions: This symptom is observed with MVPN with 500 VRFs, when performing multiple switchovers on PE1.

  Workaround: There is no workaround.

- CSCub87579

  Symptoms: Multicast traffic gets forwarded to the wrong tunnel protected with IPsec.

  Conditions: This symptom is observed when Multicast (PIM) is enabled on the GRE tunnel protected with IPsec on the Cisco 7600.

  Workaround: Shut/no shut on the tunnel protected with IPsec resolves the issue.

- CSCub88742

  Symptoms: A crash occurs due to NULL pointer access in a BGP C-Route function.

  Conditions: This symptom is very timing-sensitive and occurs only in a specific sequence of runtime events at a specific timing instance. In this case, it is triggered on a scaled setup when “mpls mldp” is toggled after two SSOs and when each SSO takes a very long time to complete due to HA Bulk Sync failure in IP Multicast that has addresses separately.

  Workaround: There is no workaround.

- CSCub89711

  Symptoms: The **atm** keyword for the **show** command disappears.

  Conditions: This symptom occurs when you do a powered shutdown of the SPA card and bring it back up using the **no** form the previous command.

  Workaround: There is no workaround.

- CSCub91428

  Symptoms: Internal VLAN is not deleted even after waiting for 20 minutes, and the VLAN cannot be reused.

  Conditions: This symptom is seen with any internal VLAN allocated dynamically that is not freed up after 20 minutes in the pending queue.

  Workaround: There is no workaround.

- CSCub91429

  Symptoms: CEF does not get programmed and traffic does not flow across IPv6 VTI tunnels post router reload.

  Conditions: This symptom occurs when reloading the box that has scale IPv6 sVTI IPsec tunnels configured.

  Workaround: Shutdown/no shutdown on the IPv6 tunnels resolves the issue.

- CSCub91546

  Symptoms: Traffic is dropped silently on the VLAN.

  Conditions: This symptom is observed when all the VLANs in the router are used (0 free VLAN). Any new internal VLAN creation will fail, and an appropriate error message is not shown.

  Workaround: There is no workaround.

- CSCub91815

  Symptoms: Certificate validation fails with a valid certificate.

  Conditions: This symptom is observed during DMVPN setup with an empty CRL cache. This issue is usually seen on the responder side, but the initiator can also show this behavior.

  Workaround: There is no known workaround.

- CSCub94438

  Symptoms: Traceback is observed with the following error message:

  ```
  SP-STDBY: pm_get_standby_vlan:Cannot allocate VLAN for IPv6 VPN 0x1E000050 Egress
  multicast VLAN 1019 is use by Tunnel2
  ```

  Conditions: This symptom occurs when applying a scaled MLDP configuration.

  Workaround: There is no workaround.

- CSCub95141

  Symptoms: FP Pending Refs are observed when “crypto map <> local-address loopbackX” is removed from the configuration when the crypto map is applied on a subinterface.

  Conditions: This symptom is observed with the following configuration:

  ```
  crypto map cry local-address Loopback0
  interface GigabitEthernet0/0/0.100 crypto map cry
  interface GigabitEthernet0/0/0.200 crypto map cry
  ```

  Workaround: Remove “crypto map” from the subinterface first and then remove “crypto map <> local-address loopbackX”.

- CSCub98385

  Symptoms: CFMoXconnect remote MEPs are not learned.

  Conditions: This symptom is observed with CfmoXconnect on the Cisco ME3600X and TE tunnels in the core. This issue is seen when the core link is mapped to NILE 1.

Workaround: Remove TE tunnels in the core or have the core link on NILE 0.

- CSCuc05570

  Symptoms: The "PM-SP-STDBY-3-INTERNALERROR" error message is seen on Active for the Tunnel Reserved VLAN and the Tunnel Global Reserved VLAN.

  Conditions: This symptom is observed with an HA router with a scale configuration of the MDT Tunnel.

  Workaround: There is no workaround.

- CSCuc06024

  Symptoms: Traffic flowing through EVCs that do not belong to any service group will see incorrect bandwidth values because of wrong bandwidth value programmed on the port-default node.

  Conditions: This symptom is seen when a mixture of flat and HQoS SGs having bandwidth configurations on their policies are applied on PC EVCs. Two mem- links are part of this PC, and default load-balancing is used.

  Workaround: There is no workaround.

- CSCuc10586

  Symptoms: In the Cisco 7600, multicast traffic does not flow in some scenarios. In the case of PIM SM mode, many times, (*,G) is present, but not (S,G) in mroute. In the case of PIM SSM mode, (S,G) is present but still traffic does not flow through.

  Conditions: This symptom is observed only with Cisco IOS Release 15S-based releases.

  Workaround:

  - Either use a different source IP or a different group IP.
  - Reload the module.

- CSCuc10706

  Symptoms: When Cisco IOS XE is configured to use subscriber-service for authorization, it will ignore this configuration for the named list and fall back on the default for subscriber-profile or, if this is not present, on the default authorization method for the network. If none of these default authorization methods are configured, authorization will not take place.

  Conditions: This symptom occurs when a named authorization list is configured.

  Workaround: Set the default authorization list (subscriber-service or network) to use the correct Radius server.

- CSCuc11853

  Symptoms: T1 controller will stay DOWN after switchover.

  Conditions: This symptom is seen when SATOP is configured on T1.

  Workaround: Do a shut and no shut.

- CSCuc13992

  Symptoms: The Cisco IOSd process crashes due to a segmentation fault in the PPP process:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = PPP Events
  ```

  The root cause for the PPP process crash is wrong IPCP option processing inside PPP control packets.

  Conditions: This symptom occurs when the BRAS functionality is configured, which includes ISG and PPPoE session termination.

Workaround: There is no workaround.

- CSCuc14088

  Symptoms: The default class is not being exported with the class option template.

  Conditions: This symptom occurs when class-default is not exported when typing the option c3pl-class-table under the flow exporter.

  Workaround: There is no workaround.

- CSCuc15810

  Symptoms: MVPN over GRE PIM VRF neighbor is not up after SSO.

  Conditions: This symptom is seen when MVPN over GRE PIM VRF neighbor is not up after SSO.

  Workaround: There is no workaround.

- CSCuc28757

  Symptoms: IPv6 HbH Traffic traversing across BD SVIs will not be rate-limited by HbH rate-limiter that is configured.

  Conditions: This symptom is seen when enabling HbH rate-limiter on an NP of ES+ and IPv6 HbH traffic traversing across SVIs part of EVC BD of ES+ interface.

  Workaround: There is no workaround.

- CSCuc29884

  Symptoms: Outage and CPU remain astonishingly high against XDR MCAST process on a scaled HWO BFD testbed.

  Conditions: This symptom is seen after a router reload, when OSPF converge is getting completed, and started 10g traffic through the box.

  Workaround: There is no workaround.

- CSCuc29966

  Symptoms: Traffic loss is seen on switchover over interfaces on TDM IM.

  Conditions: This symptom occurs when the Cisco A900-IMA16D TDM IM crashes upon switchover.

  Workaround: There is no workaround.

- CSCuc31534

  Symptoms: With a primary PW in the down state, if the Xconnect redundancy configuration is removed and added, then switching may remain down and the VC goes down.

  Conditions: This symptom is observed with the following conditions:

  1. The platform supports hot standby (Cisco ASR 903/Cisco 7600/Cisco ASR 901).
  2. PW redundancy with primary down.
  3. Configuration removed + added or added afresh.

  Workaround: Fix the primary PW and then remove/add the configuration.

- CSCuc34088

  Symptoms: The router passes lower traffic levels when you add links to an IMA bundle and perform IM OIR/router reload.

  Conditions: This symptom occurs when you send traffic above the E1 line rate on one link within an IMA bundle and perform IM OIR.

Workaround: Removing and re-applying the IMA interface brings it back up

- CSCuc34574

  Symptoms: A pending-issue-update is seen at SSL CPP CERT on the Cisco ASR 1002, ESP-1000 platform.

  Conditions: This symptom is observed with the following configuration:

```
show platform software object-manager fp active pending-issue-update

Update identifier: 128
  Object identifier: 117
  Description: SSL CPP CERT AOM show
  Number of retries: 0
  Number of batch begin retries: 0
```

  Workaround: There is no workaround.

- CSCuc35935

  Symptoms: Traffic coming in with a particular label might experience drops on ES+.

  Conditions: This symptom is observed with traffic coming in on the ES+ interface with MPLS enabled. This issue is seen when the box has AToM (Scalable mode on the Cisco 7600) configured.

  Workaround: Reset the core facing ES+ module.

- CSCuc36049

  Symptoms: The Cisco ME3600 and Cisco ME 3800 switches crash.

  Conditions: This symptom occurs on triggering POCH LACP fast switchover that is part of G.8032 ring carrying UCAST and MCAST traffic.

  Workaround: There is no workaround.

- CSCuc36522

  Symptoms: The router does not timestamp traffic on port-channel interfaces.

  Conditions: This symptom cccurs when you configure a CFM EVC bridge-domain up MEP on a port-channel.

  Workaround: There is no workaround.

- CSCuc37047

  Symptoms: VSS crashes on reconfiguring “ipv6 unicast-forwarding” multiple times.

  Conditions: This symptom occurs when CTS is configured on an interface and “ipv6 unicast” is toggled multiple times.

  Workaround: There is no workaround.

- CSCuc38446

  Symptoms: The upgrade for Handoff FPGA from version 3000F to 30017 fails.

  Conditions: This symptom is observed when upgrading Handoff FPGA.

  Workaround: There is no workaround.

- CSCuc38851

  Symptoms: DHCP snooped bindings are not restored after an RTR reload.

  Conditions: This symptom might occur when bindings are learnt on Cisco ES20 EVCs.

  Workaround: After the RTR is UP, renew from the agent database by issuing the **renew ip dhcp snooping database** *URL* command.

- CSCuc41369

  Symptoms: Complete traffic loss occurs for V6 mroutes.

  Conditions: This symptom occurs during deletion and addition of VRFs for the MVPNv6 inband signaling configuration.

  Workaround: There is no workaround.

- CSCuc41879

  Symptoms: Multicast traffic for few mroutes gets dropped on the bud node. This issue occurs as sub-LSPs are not created due to LSP IDs getting exhausted.

  Conditions: This symptom occurs after reload, TE-FRR, and churning of mroutes.

  Workaround: There is no workaround.

- CSCuc42002

  Symptoms: The router crashes when configuring the ATM interface.

  Conditions: This symptom is observed with the following sequence:

  1. Move OC3 IM with the ATM configuration to a different bay.
  2. Configure an ATM interface on the new bay.
  3. Cisco IOSd crash is seen due to a segmentation fault.

  Workaround: There is no workaround.

- CSCuc42117

  Symptoms: The router does not include 0xff03 flag leading bits within ppp fragment messages.

  Conditions: This symptom occurs when the router has not negotiated ACFC.

  Workaround: There is no workaround. Most remote devices should ignore this behavior by design, but some devices may display unexpected behavior, such as for IPCP PROTREJ messages.

- CSCuc44555

  Symptoms: Multicast traffic is not forwarded to downstream, even when the groups show up in the group list.

  Conditions: This symptom is observed only when the traffic comes on RPF fail interface, and the downstream port is blocked due to STP or similar protocol.

  Workaround: Disable IGMP snooping.

- CSCuc45115

  Symptoms: EIGRP flapping is seen continuously on the hub. A crash is seen at nhrp_add_static_map.

  Conditions: This symptom is observed after shut/no shut on the tunnel interface, causing a crash at the hub. A related issue is also seen when there is no IPv6 connectivity between the hub and spoke, causing continuous EIGRP flapping on the hub.

  Workaround: There is no known workaround.

- CSCuc45528

  Symptoms: Incremental leaks are seen at :__be_nhrp_recv_error_indication.

  Conditions: This symptom occurs when the NHRP error indication is received on the box. This issue is seen only if CSCub93048 is already present in the image. CSCub93048 is available from Cisco IOS Release 15.3M&T onwards.

Workaround: There is no workaround.

- CSCuc46356

  Symptoms: The router hangs and crashes by WDOG.

  Conditions: This symptom occurs when IPv6 ACL is applied to a port-ch sub-if. The sub-if is deleted followed by deletion of the ACL.

  Workaround: Delete the ACL before deleting the port-ch sub-if.

- CSCuc47399

  Symptoms: IKEv2 STOP Accounting records show wrong counters for packets/octets, when the sessions are locally cleared using “clear crypto sa” or “clear crypto session”.

  Conditions: This symptom is observed with the latest Cisco IOS XE Release 3.8S images when IKEV2-Accouting is enabled. This issue is easily reproducible with a single session, and may be service impacting as STOP Accounting records are usually used for billing purposes.

  Workaround: The STOP records reflect the right counters when the disconnect is through the remote end.

- CSCuc48162

  Symptoms: EVC Xconnect UP MEP is sending CCMs when the remote EFP is shut.

  Conditions: This symptom occurs when EFP is admin down.

  Workaround: There is no workaround.

- CSCuc48211

  Symptoms: Traffic from the Label Edge Router (LER) is dropped at the Label Switch Router (LSR) peer. LER is using a invalid/outdated label, unknown to LSR. This issue can be seen with a regular MPLS connection over a physical interface or with a connection over an MPLS TE tunnel interface. The root cause is that LER is using CEF long-path extension, installed to the prefix by a different routing protocol in the past.

```
TUNNEL-HEADEND/LER#show ip cef 172.25.0.1 internal
172.25.0.0/16, epoch 6, flags rib only nolabel, rib defined all labels, RIB[B],
refcount 5, per-destination sharing
  sources: RIB
  feature space:
   IPRM: 0x00018000
   Broker: linked, distributed at 4th priority
   LFD: 172.25.0.0/16 0 local labels
        contains path extension list
  ifnums:
   TenGigabitEthernet1/0/0(31): 10.10.243.48
   Tunnel11(38)
  path 1F13EC1C, path list 1436FC80, share 1/1, type recursive, for IPv4
  recursive via 10.10.254.3[IPv4:Default], fib 21B2A5CC, 1 terminal fib,
v4:Default:10.10.254.3/32
    path 13A71668, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
      MPLS short path extensions: MOI flags = 0x1 label 1683
    nexthop 10.10.243.48 TenGigabitEthernet1/0/0 label 1683, adjacency IP adj
out of TenGigabitEthernet1/0/0, addr 95.10.243.48 20BCED00
    path 13A745A8, path list 20C50DB0, share 1/1, type attached nexthop, for IPv4
      MPLS short path extensions: MOI flags = 0x1 label 623
      MPLS long path extensions: MOI flags = 0x1 label 18
    nexthop 10.10.255.130 Tunnel11 label 18, adjacency IP midchain out of
Tunnel11 22923160
  long extension for path if Tunnel11 next hop 10.10.255.130:
    MPLS long path extensions: MOI flags = 0x1 label 18
  long extension for path if Tunnel22 next hop 10.10.255.129:
```

```
    MPLS long path extensions: MOI flags = 0x1 label 651
  output chain:
    loadinfo 212F8810, per-session, 2 choices, flags 0083, 4 locks
    flags: Per-session, for-rx-IPv4, 2buckets
    2 hash buckets
      < 0 > label 1683 TAG adj out of TenGigabitEthernet1/0/0, addr
10.10.243.48 20BDC860
      < 1 > label 18 TAG midchain out of Tunnel11 20C92B00 label implicit-null
TAG adj out of TenGigabitEthernet1/0/1, addr 10.10.243.50 20B21440
    Subblocks:
     None

TUNNEL-TAILEND/LSR# sh mpls forwarding-table labels 18
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
TUNNEL-TAILEND#
```

Conditions: This symptom occurs when the prefix is learned by both BGP and IGP, while BGP has lower Administrative Distance, pointing via the MPLS TE tunnel carrying MPLS. This issue is seen once the prefix is installed to RIB by IGP and then by BGP (Reload, BGP flap, etc.); then, the CEF will keep using the IGP/LDPs label without updating it in case of LDP label change.

Workaround: Issue the **clear ip route** *prefix mask* command.

- CSCuc49967

  Symptoms: Router crash points to the “IP SLAs XOS Event Processor” process and decodes point to “ecfm_pal_pd_encap_pak”.

  Conditions: This symptom occurs when configuring IPSLA sessions with a Mac-Address that is not present in the CFM CCDB.

  Workaround: This issue is not seen when Mac-Addresses are learned in CCDB.

- CSCuc51692

  Symptoms: The router crashes while enabling L2TP debugs using the **debug l2vpn l2tp error | event** command.

  Conditions: This symptom always occurs on enabling the **debug l2vpn l2tp error | event** command.

  Workaround: The same debugs can be enabled using the alternate command **debug xcl2 error | event**.

- CSCuc52506

  Symptoms: 6PE and 6VPE traffic drops on shutting the ECMP link.

  Conditions: This symptom occurs after configuring the 6PE/6VPE between UPE-2 and UPE-1 with ECMP paths between both nodes and then shutting the ECMP link.

  Workaround: There is no workaround.

- CSCuc53135

  Symptoms: LDP sessions are not established.

  Conditions: This symptom is observed on a router with more than one LDP adjacency to a neighbor. This issue is seen when the TCP session establishment to that neighbor is delayed, and while it is delayed, the adjacency that is the active adjacency times out (no more UDP packets are received), resulting in the TCP listen socket being deleted and not created.

  Workaround: Issue the **clear mpls ldp neighbor *** command.

- CSCuc56259

  Symptoms: A Cisco 3945 that is running 15.2(3)T2 and running as a voice gateway may crash. Just prior to the crash, these messages can be seen:

  ```
  %VOIP_RTP-6-MEDIA_LOOP: The packet is seen traversing the system multiple times
  ```

  and

  ```
  Delivery Ack could not be sent due to lack of buffers.
  ```

  Conditions: This symptom occurs when a media loop is created (which is due to misconfiguration or some other call forward/transfer scenarios).

  Workaround: Check the configurations for any misconfigurations, especially with calls involving CUBE and CUCM.

- CSCuc57130

  Symptoms: Interface configurations do not work post HA switchover.

  Conditions: This symptom occurs after HA switchover and is observed with OC3 IM.

  Workaround: There is no workaround.

- CSCuc59049

  Symptoms: The Cisco ME3800x crashinfo files may be incomplete.

  Conditions: This symptom occurs when a crashinfo file is created when a crash occurs.

  Workaround: Gather console logs and syslogs to help troubleshoot crashes.

- CSCuc59105

  Symptoms: The switch may crash when issuing “show platform qos policer cpu x x”.

  Conditions: This symptom occurs only when issuing “show platform qos policer cpu x x” through an SSH session with AAA configured.

  Workaround: Execute the command through Telnet or the console.

- CSCuc64719

  Symptoms: A Cisco ME 3600X HSRP failover is seen in VPLS.

  Conditions: This symptom occurs when HSRP state changes from active to standby. The MAC address on the active router is not flushed.

  Workaround: Clear the MAC table on the HSRP active router.

- CSCuc66895

  Symptoms: Layer 2 traffic loop seen in REP topology for a transient time, when the Cisco ASR 903 which is a part of the REP ring is reloaded.

  Conditions: This symptom is observed when the Cisco ASR 903 is part of an REP ring, and the box is reloaded with saved REP configurations.

  Workaround: Traffic loop is transient, once REP convergence looping is stopped.

- CSCuc67687

  Symptoms: With a rare combination, and VRF-related RG configurations, the router may crash following the configuration commands.

  Conditions: This symptom is observed with the following configuration:

  ```
  R1-13RU(config-if)#ip vrf forwarding b2b-vrf
  % Interface GigabitEthernet0/1/0 IPv4 disabled and address(es) removed due to
  ```

```
enabling VRF b2b-vrf
% Interface GigabitEthernet0/1/0 virtual IP address <ip> removed due to VRF change
% Zone security Z1 is removed due to VRF config change on interface
GigabitEthernet0/1/0

R1-13RU(config-if)#ip address <ip> <mask>
R1-13RU(config-if)#zone-member security Z1
R1-13RU(config-if)#redundancy group 1 ip <ip> exc dec 50
```

Workaround: There is no known workaround.

- CSCuc68246

  Symptoms: The standby IOMD crashes on booting up the standby RSP.

  Conditions: This symptom occurs when booting up the standby RSP with a configuration that is already present.

  Workaround: Boot up the standby without any configurations and start configuration once the standby has reached STANDBY_HOT state.

- CSCuc71706

  Symptoms: Execution of the **show run** command and other commands such as **copy run start** and **show access-list** cause the router to stop for a few minutes before completing.

  Conditions: This symptom is observed with Cisco ISR G2 routers. This issue is seen only with IPV6 configured and used.

  Workaround: There is no workaround.

- CSCuc72244

  Symptoms: On the Cisco 7609, both sides running Cisco IOS Release SRE4 SIP-400 with SPA-2X1GE-V2 configured with “negotiation Auto” and changed to “no negotiation auto”. The GE interface of the router is operating in half-duplex mode after falling back. The interface is operating in half-duplex instead of the expected (nonconfigurable) full-duplex.

  Conditions: This symptom does not occur under any specific conditions. This issue is observed due to a timing constraint upon updating the duplex state.

  The steps to reproduce are as follows:

  1. The interface in Router A is configured to “negotiation auto” with no change in duplex state on both sides.
  2. The interface in Router B is configured to “negotiation auto” with no change in duplex state on both sides.
  3. The interface in Router A is configured to “no negotiation auto”. The duplex state for both interfaces is changed to half-duplex.
  4. The interface in Router B is configured to “no negotiation auto”. The interface duplex state for Router B is changed to full-duplex. But, the Router A interface remains in half-duplex.

  Workaround: There is no workaround.

- CSCuc72594

  The Cisco IOS Software implementation of the IP Service Level Agreement (IP SLA) feature contains a vulnerability in the validation of IP SLA 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. Mitigations for this vulnerability are available.

  This advisory is available at the following link:

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

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

- CSCuc76670

  Symptoms: 2X1GE-SYNCE (metronome) SPA does not boot on a 2RU (Cisco ASR 1002).

  Conditions: This symptom is observed with Cisco IOS XE Release 3.7S onwards, when metronome SPA (2X1GE-SYNCE) fails to boot on a 2RU. An error message indicating that the SPA is not supported is displayed on the RP console.

  Workaround: There is no workaround.

- CSCuc77283

  Symptoms: Upon reload or OIR, the CFM MEP configuration on an xconnect EFP is removed and cannot be reconfigured.

  Conditions: This symptom is observed with a CFM MEP on xconnect service instance. This issue is seen when reload or OIR is performed.

  Workaround: Remove the domain configuration.

- CSCuc77704

  Symptoms: The GETVPN/GDOI Secondary Cooperative Key Server (COOP-KS) does not download the policy (that is, when the **show crypto gdoi ks policy** command is issued on the Secondary COOP-KS and the command output shows that no policy is downloaded) and Group Members (GMs) registering to the Secondary COOP-KS fail to register without any warning/error message.

  Conditions: This symptom is observed when the GETVPN/GDOI group (with COOP configured) has an IPsec profile configured with one of the following transforms in its transform-set:

  - esp-sha256-hmac
  - esp-sha384-hmac
  - esp-sha512-hmac

  Workaround: Use esp-sha-hmac as the authentication transform instead.

- CSCuc79161

  Symptoms: Memory leak is observed.

  Conditions: This symptom occurs after flapping the interface, keeping the setup idle, and executing "clear xconnect".

  Workaround: There is no workaround.

  Further Problem Description: The PI front-end pseudoport is not deleted when the xconnect is removed, which causes the memory leak. This issue occurs because PD returns BDOMAIN_PP_FAILED to PI when pp_engine_context is a NULL pointer.

- CSCuc79923

  Symptoms: On a Cisco 7600 running Cisco IOS Release 15.2(4)S1, packets from FWSM are dropped when the servicemodule session is enabled. Ping fails for the VLAN interface on the FWSM module from the supervisor. The ARP entry is incomplete on the Cisco 7600.

  Conditions: This symptom is observed with the following conditions:

  - This issue is seen on the Cisco 7600 with FWSM and SUP-720-3B running Cisco IOS Release 15.2(4)S1.
  - The FWSM is in Crossbar mode.
  - The system is in “distributed” egress SPAN replication mode.

  This issue is not seen with Cisco IOS Release 12.2(33)SRE7.

  Workaround:

  - Disable the servicemodule session.
  - Change the fabric switching mode to bus.
  - Change SPAN egress replication mode to “centralized”.

- CSCuc82551

  Symptoms: A Cisco ASR 1001 running Cisco IOS XE Release 3.6.2S or Cisco IOS XE Release 3.7.1S crashes with SNMP traffic.

  Conditions: This symptom is observed with SNMP polling with an IP SLA configuration.

  The crash signature is as follows:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = SNMP ENGINE
  ```

  Workaround: Remove the SNMP configuration from the router or schedule the probe before polling via SNMP.

- CSCuc91582

  Symptoms: Adding EFP to Bridge-Domain fails and errors are seen when reloading with Cisco IOS XE Release 3.7.1a.

  Conditions: This symptom is observed when reloading the Cisco ASR 903 with Cisco IOS XE Release 3.7.1a, when EFP and PW are in the same Bridge-Domain.

  Workaround: Post reload, remove the EFP configurations, and configure PW first and then EFP.

- CSCuc97711

  Symptoms: After SSO, traffic on the P2P-GRE tunnel within an MVPN may be affected.

  Conditions: This symptom is observed with Cisco IOS Release SREx- and RLSx-based releases.

  Workaround: Shut/no shut the P2P tunnel interface.

- CSCuc98226

  Symptoms: When a PC is moved between two VLAN ports (on one port, ISG is enabled, and the other is non-ISG) several times by its LAN cable connection on the L2SW that is connected to the Cisco ASR 1000 router, the PC becomes unable to acquire an IP address from DHCP on the router. At that time, an incorrect interface is shown in “show ip dhcp binding”.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(4)S1.

  Workaround: There is no workaround.

- CSCuc98590

  Symptoms: The router can crash on removal of the boundary clock (BC). configuration.

  Conditions: This symptom is observed upon removal of the BC configuration. This issue is seen very rarely, and there is no other specific trigger.

  Workaround: There is no workaround. The chances of encountering this issue have been found to be remote as it is seen rarely.

- CSCud03877

  Symptoms: After volume rekey, the IPsec PD flow sets both the hard and soft limit of the traffic limit to 0.

  Conditions: This symptom is observed when the volume rekey is set to 0.

  Workaround: Clear crypto session to recover the volume rekey value.

- CSCud07856

  Symptoms: SP crashes at “cfib_update_ipfrr_lbl_ref_count”.

  Conditions: This symptom is observed with a scaled IP-FRR configuration.

  Workaround: Remove the IP-FRR configuration.

- CSCud16693

  Symptoms: The Cisco ME3600X/ME3800X switch crashes as soon as you apply policy-map referencing table-map.

  Conditions: This symptom occurs when applying a service policy which has an unsupported combination of police action with table-map and without table-map.

  Workaround: Configure a service policy which does not have the combination of police action with table-map and without table-map.

- CSCud17934

  Symptoms: PW redundancy on the Cisco 7600 does not work when the primary VC goes down and the backup VC takes over, and CE to CE communication is broken.

  Conditions: This symptom is observed with the following conditions:

  - The MPLS facing LC is WS-X6704-10GE.
  - The CE facing LC is ES+.

  Workaround: Use another HW on the MPLS core.

- CSCud19230

  Symptoms: ES+ line card reload occurs with the following error messages:

```
%PM_SCP-SP-1-LCP_FW_ERR: System resetting module 2 to recover from error:
x40g_iofpga_interrupt_handler: LINKFPGA IOFPGA IO Bus Err val: 4214784 Bus
Error Add:332 Bus Err
data: 0

%OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled Off (Module Reset
due to exception or
user request)

%C7600_PWR-SP-4-DISABLED: power to module in slot 2 set Off (Module Reset due
to exception or user
request)
```

  Conditions: This symptom is observed with the ES+ line card.

Workaround: There is no workaround.

- CSCud19257

  Symptoms: NAT CLIs expose the **vrf** keyword on the Cisco 7600, which is not supported.

  Conditions: This symptom is observed with a NAT configuration.

  Workaround: Do not use the **vrf** keyword for NATing on the Cisco 7600.

- CSCud22601

  Symptoms: MPLS-TP tunnels stay down.

  Conditions: This symptom occurs when the standby boots up after the TP configuration is done and SSO is performed. This issue is seen once in 100 iterations.

  Workaround: Shut/no shut the MPLS-TP tunnel. A nonintrusive workaround is to flap the protect LSP (by reconfiguring or by physical interface flap).

- CSCud24084

  Symptoms: Performing a default MDT toggling on a VRF results in the encapsulation tunnel adjacency's MTU being set to a lower MTU.

  Conditions: This symptom is observed with Cisco IOS XE Release 3.7S (Cisco IOS Release 15.2(4)S) and later releases when the mdt default <> is toggled on a VRF.

  Workaround: Delete and add the affected VRF.

  Further Problem Description: Software adjacency does not updated with the correct MTU.

- CSCud26339

  Symptoms: Changing policy-map parameters triggers a Cisco IOSd crash.

  Conditions: This symptom is observed when the policy-map is attached to a service instance on the Cisco ASR 903.

  Workaround: Remove the policy-map from the target and then make the changes.

- CSCud31012

  Symptoms: MVPNv6 does not work in the Cisco IOS XE Release 3.7S image.

  Conditions: This symptom is observed only with the IP services image.

  Workaround: Use the enterprise image.

- CSCud33028

  Symptoms: Segmentation crash occurs.

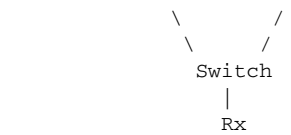
  Conditions: This symptom occurs upon executing "config replace".

  Workaround: There is no workaround.

- CSCud38004

  Symptoms: RPF failure is not supported for EFP/EVC BD. As a result, multicast traffic is not forwarded.

  Conditions: This symptom is observed in the following scenario:



Considering the above dual-home scenario, this symptom is observed when the below conditions are true:

1. N2 acts as the DR.
2. One of the dual-home links to the receiver (N2-Switch) is down.
3. EVC is configured between N1 and N2.

Workaround:

1. Move the DR to N1.
2. Use SVI between N1 and N2.

- CSCud45445

  Symptoms:

  Scenario 1: Y.1731PM does not work with “rewrite ingress tag pop 1 symmetric” at the core facing interface.

  Scenario 2: Y.1731Pm does not work on the Q-in-Q configured interface.

  Conditions: This symptom is observed with the following conditions:

  – When the core facing interface is configured as “rewrite ingress tag pop 1 symmetric”, as follows.

```
interface GigabitEthernet0/9

 switchport trunk allowed vlan none

 switchport mode trunk

 service instance 1 ethernet test

  encapsulation dot1q 151

  rewrite ingress tag pop 1 symmetric

  bridge-domain 151

 !

end
```

  – In the q-in-q configured interface, as follows.

```
interface GigabitEthernet0/1

 switchport trunk allowed vlan none

 switchport mode trunk
```

```
service instance 1 ethernet test

 encapsulation dot1q 151 second-dot1q 110

 bridge-domain 151

 cfm mep domain l7 mpid 555

  cos 1

!
```

Workaround: There is no workaround.

- CSCud48005

  Symptoms: The router crashes on applying the QoS policy-map with a classification based on ACL on the main interface.

  Conditions: This symptom is observed when you apply the policy-map on the main interface.

  Workaround: There is no workaround.

- CSCud50514

  Symptoms: DEJAVU check fails for multicast traffic for the EVC BD interface.

  Conditions: This symptom is a regression caused by bug CSCud38004. Once CSCud38004 has the complete fix, this issue will not be seen.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(4)S1

Cisco IOS Release 15.2(4)S1 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveat in this section is open in Cisco IOS Release 15.2(4)S1. This section describes only select open caveats.

- CSCtx31177

  Symptoms: RP crash is observed on avl search.

  Conditions: This crash is observed on configuration of rich system with high load. Sometimes the crash is happening when system is not being used.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S1

Cisco IOS Release 15.2(4)S1 is a rebuild release for Cisco IOS Release 15.2(4)S. The caveats in this section are resolved in Cisco IOS Release 15.2(4)S1 but may be open in previous Cisco IOS releases.

- CSCsq83006

  Symptoms: When some port-channels go down at the same time on a router, it can cause EIGRP SIA errors.

Conditions: The symptom occurs with full mesh four routers which are connected via port-channels. Additionally, it occurs with over five routers which are connected via a partial mesh port-channel.

Workaround: Use the port-channel interface settings below:

```
(config)# interface port-channel <port-channel interface number>
  (config-if)# bandwidth <bandwidth value>
  (config-if)# delay <delay value>
```

Further Problem Description: If a test is done with a physical interface, not a port-channel, this issue is not seen.

- 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

- CSCti62247

  Symptoms: If a packet is sent to a null interface, a Cisco ASR 1000 router will not respond with an ICMP packet.

  Conditions: This symptom is seen when a prefix is routed to Null0 interface.

  Workaround: There is no workaround.

- CSCto87436

  Symptoms: A Cisco device that is running Cisco IOS may crash due to a watchdog timeout with the following error messages:

```
%SYS-3-CPUHOG: Task is running for (126004)msecs, more than (2000)msecs
(30/1),process = SSH Process.
-Traceback= 0x63D827CCz 0x6496A670z 0x649774CCz 0x649776A0z 0x6497777Cz
0x6496BCFCz 0x6496BEA4z 0x6496BFF8z 0x61E122A0z 0x61DFC6CCz 0x61DFCF94z
0x61DFF270z 0x61DFC5F8z 0x61E980E0z 0x61E984ACz 0x61E3DF6Cz
%SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs
(31/1),process = SSH Process.
-Traceback= 0x63D7AA5Cz 0x62A47F68z 0x62A48500z 0x62A45F9Cz 0x649774E8z
0x649776A0z 0x6497777Cz 0x6496BCFCz 0x6496BEA4z 0x6496BFF8z 0x61E122A0z
0x61DFC6CCz 0x61DFCF94z 0x61DFF270z 0x61DFC5F8z 0x61E980E0z
 %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = SSH Process.
```

  Reason for the crash is that we are not handling the error condition properly in the call flow.

Conditions: This symptom occurs mainly due to slow response from the client. This can occur because of the below mentioned scenario. Condition that can leads to this:

Client is out of its window, and we expect window adjust message:

1. Foreign reset happens to the connection.
2. Idle timeout.
3. Timer timeout.
4. Other error to the connection.

We failed to handle this kind of error properly and we loop again and again expecting that message will come from the client even though we set the tcp->pid to No_PROCESS.

Workaround: There is no workaround. Use a stable connection and use a noise free fast underlying physical connection between the two devices.

- CSCtq17444

  Symptoms: A Cisco AS5400 crashes when performing a trunk call.

  Conditions: The following conditions are observed:

  - Affected Cisco IOS Release: 15.1(3)T.
  - Affected platforms: routers acting as voice gateway for H.323.

  Workaround: There is no workaround.

- CSCtr45287

  Symptoms: Router crashes in a scale DVTI scenario.

  Conditions: The symptom is observed when the IPsec tunnel count reaches around 2500.

  Workaround: Use fewer tunnels or use a different platform.

- CSCts54641

  Symptoms: Various small, medium, or big VB chunk leaks are seen when polling EIGRP MIB or during SSO.

  Conditions: This symptom is observed when MIBs are being polled or SSO is done.

  Workaround: There is no workaround.

- CSCtw88689

  Symptoms: A crash is seen while applying the policy map with more than 16 classes with the Cisco 3900e platform.

  Conditions: This symptom occurs when applying the policy map with more than 16 classes.

  Workaround: There is no workaround.

- CSCtx23593

  Symptoms: Some virtual circuit (VC) information is missing in the Simple Network Management Protocol (SNMP) MIB object cAal5VccEntry from the output of the **snmpwal** command, but not in the router configuration command. For example, The ATM VCs 4/0.120 exist on the router but are missing in the MIB.

  Conditions: This symptom is observed on a Cisco 7204VXR (NPE-G2) router that is running Cisco IOS Release 12.2(33)SRE5 (c7200p-advipservicesk9-mz.122-33.SRE5.bin) image in the customer network. This issue may also occur in other releases.

This issue typically occurs over a period of time due to create/delete of subinterfaces. It also occurs if the customer uses the **snmp ifmib ifIndex Persist** command, which retains ifIndicies assigned to the @~@subinterfaces across router reload.

Workaround: There can be two workarounds where there is no fix present in the Cisco IOS code for this bug.

Workaround 1:

- Enter the **show atm vc** privileged EXEC command on the same device to obtain a complete list of all the VCs. Or,
- Do the SNMPWALK suffixing the ifIndex of the interface to get the value.

```
$ snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.2.1.2.2.1.2 | grep
"4/0.120"
IF-MIB::ifDescr.253 = STRING: ATM4/0.120-atm subif
IF-MIB::ifDescr.254 = STRING: ATM4/0.120-aal5 layer


$  snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.4.1.9.9.66.1.1.1.1.3 |
grep 9.9.66.1.1.1.1.3.254 ===> Got no entry of ifindex here in complete
snmpwalk
$
$ snmpwalk -v 2c -c <community> <ip address> 1.3.6.1.4.1.9.9.66.1.1.1.1.3.254
```

Doing the SNMPWALK suffixing the ifindex and getting the value can be one workaround.
SNMPv2-SMI::enterprises.9.9.66.1.1.1.1.3.254.200.106 = Counter32: 403633041

Workaround 2:

1. Under configuration mode: no snmp ifmib ifIndex Persist.
2. On all the ATM main interfaces: no snmp ifindex persist.
3. Save the configuration: copy running start.
4. Reload the box: reload. Reapply the persist configurations.
5. Configure in configuration mode: snmp ifmib ifIndex Persist.
6. Under the ATM main interface: snmp ifindex persist.

After this workaround, the problem may reappear over a period of time, but chances are very less.

The workaround/fix which needs to be enabled where the code fix is present in the Cisco IOS code for this bug.

Since this will go over all the possible ifIndicies, it will take more CPU cycles, causing some delay. The below global CLI can be used to enable/disable the fix based on the need.

CLI: snmp-server enable traps atm snmp-walk-serial

- CSCtx54882

  Symptoms: A Cisco router may crash due to Bus error crash at voip_rtp_is_media_service_pak.

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 15.1(4)M2.

  Workaround: There is no known workaround.

- CSCtx80535

  Symptoms: DHCP pool that is configured for ODAP assigns the same IP to multiple sessions.

Conditions: PPP users receive pool via Radius. The pool is defined on the Cisco 10000 series router to use ODAP. ODAP is receiving the subnets from Radius correctly, and assigns IPs to PPP sessions, but sometimes two users end up having the same IP address.

Workaround: Clear both sessions sharing the same IP.

- CSCtx89615

  Symptoms: Classification on the switchport interface will not work on reload of the box.

  Conditions: This symptom occurs when reloading the box.

  Workaround: Remove the policy-map and apply it back.

- CSCty01237

  Symptoms: The router logs show:

  ```
  <timestamp> %OER_BR-5-NOTICE: Prefix Learning STARTED CMD: 'show run' <timestamp>
  ```

  This is followed by the router crashing.

  Conditions: This issue is seen under the following conditions:

  1. Configure PfR with a learn-list using a prefix-list as a filter and enable learn.
  2. Use a configuration tool, script or NMS that periodically executes **show run** on the MC over HTTP or some other means.

  Workaround 1: If you use PfR learn-list feature, do not execute **show run** periodically.

  Workaround 2: If you use a monitoring tool that executes **show run** periodically, avoid using a learn-list configuration in PfR.

- CSCty07558

  Symptoms: DHCPv6 packets are dropped on a Cisco 7600 switch. For example, they are not flooded.

  Conditions: This symptom is observed when there is no IPv6 address on an SVI or if l2 VLAN has SVI in shut state (default existence after a new ACL feature).

  Workaround: Two possible workarounds which essentially serve as the fix due to the limitations they impose:

  1. When working with a pure L2 VLAN, remove ttl rate limiter (selected as default rate limiter on Cisco7600, but not on other boxes) using “no mls rate-limit all ttl-failure”.
  2. If the design permits and TTL rate limiter is necessary, put a dummy IPv6 address on the SVI or simply configure IPv6 enable on the SVI.

- CSCty12312

  Symptoms: Multilink member links move to an up/down state and remain in this condition.

  Conditions: This symptom occurs after multilink traffic stops flowing.

  Workaround: Remove and restore the multilink configuration.

- CSCty30952

  Symptoms: QoS policy-map gets rejected on shut/no shut of the interface or when the router reloads.

  Conditions: This symptom occurs when the router reloads or shut/no shut of the interface.

  Workaround: Apply the policy-map back.

- CSCty35726

  Symptoms: The following is displayed on the logs:

`InterOp:Cube-NavTel : LTI: Video Xcode Call with plain Audio FAILS`

Conditions: This symptom is seen when video Xcode call with plain audio fails.

Workaround: There is no workaround.

- CSCty41336

  Symptoms: Forward-alarm ais does not work on CESoPSN circuits.

  Conditions: This symptom occurs when you create SAToP and CESoPSN circuits and configure "forward-alarm ais".

  Workaround: There is no workaround.

- CSCty59891

  Symptoms: On the node where shut/no shut is issued, traffic does not reach IPsec VSPA, which is supposed to get encrypted.

  Conditions: This symptom is observed when issuing shut/no shut on the GRE tunnel protected with IPsec and QoS configured on this IPsec tunnel.

  Workaround: Remove and attach “tunnel protection ipsec profile”.

- CSCty64216

  Symptoms: On unconfiguring a scaled ACL, the router crashes.

  Conditions: This symptom is observed when an ACL having 1000 ACEs or more is unconfigured.

  Workaround: There is no workaround.

- CSCty64255

  Symptoms: BGP L3VPN dynamic route leaking feature from the VRF to global export feature, the prefix-limit is incorrect upon soft clear, or new prefix added, or prefix deleted.

  Conditions: This symptom is observed when VRF to global export is enabled, and prefix-limit is configured.

  Workaround: BGP hard clear.

- CSCty65189

  Symptoms: Incoming register packets are dropped at the RP when zone-based firewall (ZBFW) is configured on the RP.

  Conditions: The symptom is observed when ZBFW is configured.

  Workaround: There is no workaround.

- CSCty79284

  Symptoms: Source connected to dual home node is not forwarded to receivers in PIM SSM mode. The issue was due to the PIM joins not reaching the source node.

  Conditions: This symptom occurs with dual home node with PIM SSM with traffic source.

  Workaround: Add static group to forward the traffic to next hop router.

- CSCty80541

  Symptoms: Having EVC BD, with split-horizon group as 0 or 2 as CE-facing, drops the traffic over VPLS core pseudowire (split-horizon enabled).

  Conditions: This symptom is observed when CE-facing interface is EVC BD with split-horizon group as 0 or 2. For split-horizon group 1, traffic flows fine. The issue with CE-facing as group 0, cannot be fixed because of hardware limitation.

  Workaround: There is no workaround.

- CSCty86039

  Symptoms: Shut down the physical interface of tunnel source interface. The router crashes with traffic going through some of the tunnels.

  Conditions: This symptom is seen with tunnel interface with QoS policy installed.

  Workaround: There is no workaround.

- CSCty89224

  Symptoms: A Cisco IOS router may crash under certain circumstances when receiving a mvpnv6 update.

  Conditions: This symptom is observed when receiving mvpnv6 update.

  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-2012-3895 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

- CSCtz00430

  Symptoms: The static route is removed from the routing table.

  Conditions: This symptom is observed when pulling out and replacing a connection to the management interface.

  Workaround 1: Default the management interface and reconfigure IP.

  Workaround 2: Do a shut and no shut on the management interface through the CLI.

- CSCtz07419

  Symptoms: The PTP session is PHASE_ALIGNED for a day, and then the PTP master crashes.

  Conditions: This symptom is seen during longevity run.

  Workaround: There is no workaround.

- CSCtz12525

  Symptoms: Accounting stop is sent without Acct-Input-Packets Acct-Output-Packets Acct-Input-Octets Acct-Output-Octets when service stop is performed.

  Conditions: This symptom is observed when service stop is issued for the prepaid service.

  Workaround: There is no workaround.

- CSCtz16798

  Symptoms: On configuring "ip pim snooping" on a L3 MCAST box, crash is observed.

  Conditions: This symptom when L2 specific functionality is enabled on a L3 box. This is more of an unsupported and undesired configuration as the L3 box is capable of building the MCAST database on its own.

  Workaround: Do not configure "ip pim snooping" on L3 Cisco ME 3600X and ME 3800X boxes.

- CSCtz17977

  Symptoms: Not able to ping HSRP VIP address over Routed VPLS.

Conditions: This is seen when two Cisco ME 3600s (me360x-universalk9-mz.152-2.S.bin) are connected together via VPLS. The Cisco ME 3600X-1 is configured with HSRP under VLAN50, and the R1 is able to ping. The R2 and Cisco ME 3600X-2 are not able to ping the VIP (HSRP) address. The R2 and Cisco ME 3600X-2 are able to ping physically the IP address of R1 and the Cisco ME 3600X-1. We do have ARP entry for the VIP address on all routers.

-----VPLS--------- R1(fa0/1)--------Vlan50 ME3600X-1-0/2--------Ten-------0/2-ME3600X-2-Vlan50-- -----fa0/1-R2

Workaround: There is no workaround.

- CSCtz26683

  Symptoms: An unsupported “ip verify unicast ...” configuration applied to an interface may still be shown in **show running-config** after being rejected. Output similar to the following will appear when applying the configuration:

```
% ip verify configuration not supported on interface Tu100
  - verification not supported by hardware
% ip verify configuration not supported on interface Tu100
  - verification not supported by hardware
%Restoring the original configuration failed on Tunnel100 - Interface Support
Failure
```

  Conditions: This occurs when there is no prior “ip verify unicast ...” configuration on the interface and when the interface and/or platform do not support the given RPF configuration.

  Workaround: In some cases it may be possible to get back to the previous configuration by using a **no** form of the command. In other cases, it will be necessary to reload the device without saving the configuration, or editing the configuration manually if already saved.

- CSCtz37164

  Symptoms: The requests to the RADIUS server are retransmitted even though the session no longer exists, causing unnecessary traffic to RADIUS, and RADIUS getting requests for an invalid session.

  Conditions: This symptom occurs when the RADIUS server is unreachable and the CPE times out the session.

  Workaround: The fix is currently being worked upon. This issue can be seen as per the conditions mentioned above. This issue can be avoided by making sure that the RADIUS server is always reachable.

- CSCtz43626

  Symptoms: Minor or major temperature alarms reported in the syslog:

```
%C7600_ENV-SP-4-MINORTEMPALARM: module 2 aux-1 temperature crossed threshold
#1(=60C). It has exceeded normal operating temperature range.
%C7600_ENV-SP-4-MINORTEMPALARM: EARL 2/0 outlet temperature crossed threshold
#1(=60C). It has exceeded normal operating temperature range.
```

  Conditions: This symptom is observed on ES+ series line cards of Cisco 7600 series routers. Specifically, reported temperature will be far off from reading of other sensors on the line card.

  Workaround: There is no workaround.

  Further Problem Description: This is en enhancement in temperature reading on ES+ line cards of Cisco 7600 series routers. Reading of any temperature sensor is compared to its adjacent sensors. If the reading deviates too much from adjacent sensors, this reading is ignored. This enhancement is eliminating the single point of failure, by which one faulty sensor can trigger an environmental alarm. Nature of heat dissipation and the number and placement of temperature sensors on ES+ line cards allow for such logic to be introduced.

- CSCtz44989

  Symptoms: A EIGRP IPv6 route redistributed to BGP VRF green is not exported to VRF RED. Extranet case is broken for IPv6 redistributed routes.

  Conditions: The issue is seen with IPv6 link-local nexthop. When the EIGRP route is redistributed to BGP VRF, it clears the nexthop information (it become 0.0.0.0). Now this route becomes invalid and BGP is not able to export to another VRF.

  Workaround: There is no workaround.

- CSCtz48338

  Symptoms: A router may crash with setup with configuration of BGP L3VPN VRF to global export, NSR, and large scale, hard clear or link flap.

  Conditions: This symptom is seen under the following conditions:

  1. BGP L3VPN VRF to global import
  2. NSR
  3. Large scale

  Workaround: There is no workaround.

- CSCtz50204

  Symptoms: A crash is observed on EzVPN Server if VRF configuration under the ISAKMP profile is modified.

  Conditions: The crash is observed only if there are active sessions at the time of configuration change.

  Workaround: Prior to applying a configuration change, clear the sessions.

- CSCtz58941

  Symptoms: The router crashes when users execute the **show ip route XXXX** command.

  Conditions: This symptom is observed during the display of the **show ip route XXXX**, when the next-hops of “XXXX” networks are removed.

  Workaround: The **show ip route XXXX** command (without “XXXX”) does not have the problem.

- CSCtz61556

  Symptoms: ATM local switching segments do not come up after changing encap on both interfaces.

  Conditions: This symptom is seen with ATM VC local switching. If the encap on both the ATM VC segments are changed, the segments remain in DOWN state.

  Workaround: There is no workaround.

- CSCtz71084

  Symptoms: When the prefix from CE is lost, the related route that was advertised as best-external to RR by PE does not get withdrawn. Even though the BGP table gets updated correctly at PE, RIB still has a stale route.

  Conditions: This symptom is observed with a topology like shown below, where CE0 and CE1 advertise the same prefixes:

  CE0----------PE0----------RR | | | | CE1----------PE1----------|

  Best-external is configured at PEs. PE0 prefers the path via PE1 and chooses it as its best path and advertises its eBGP path as the best-external path to RR. RR has two routes to reach the prefix, one via PE0 and the other via PE1. This issue occurs when CE0 loses the route; therefore, PE0 loses its best-external path and it has to withdraw, but this does not happen.

This issue does not occur if the interface between PE0-CE0 is shut from either side. Instead, the following command should be issued to stop CE0 from advertising the prefix: no network x.x.x.x mask y.y.y.y

Even though the trigger has SOO, it is not necessary for the repro. This same issue can be observed by PIC (stale backup path at RIB under the similar scenario), diverse-path, and inter-cluster best-external, and is day 1 issue with all.

Workaround: Hard clear.

- CSCtz83221

  Symptoms: Active or standby route processor crashes.

  Conditions: This symptom can be seen during the configuration or removal of ATM virtual circuits.

  Workaround: There is no workaround.

- CSCtz92606

  Symptoms: MFR memberlinks-T1 serial interfaces created under a CHOC12 controller, do not get decoupled from MFR even after the MFR bundle interface is deleted. Once the MFR bundle interface is reconfigured, the memberlinks do not appear under it.

  Conditions: This symptom is seen with MFR with memberlinks as T1 serials from CHOC12 sonet controller.

  Workaround: Unconfigure and reconfigure the “encap frame-relay MFRx” under each memberlink after reconfiguring the MFR bundle interface.

- CSCtz94902

  Symptoms: Memory allocation failure is seen when attaching to SIP-40 using a web browser.

  Conditions: This symptom is seen on the line card with a memory allocation failure.

  Workaround: Reset the line card.

- CSCtz96504

  Symptoms: Some of the backup VCs are down after SSO.

  Conditions: This symptom happens only on scale scenario where 500 primary and 500 backup VCs were created.

  Workaround: These backup VCs can be brought to SB state by issuing the **clear xconnect peerid** p*eerid of the PW* **vcid** *vcid* command. Although it is not usually recommended, it is the only way to recover.

- CSCua06598

  Symptoms: Router may crash with breakpoint exception.

  Conditions: The symptom is observed when SNMP polls IPv6 MIB inetCidrRouteEntry and there is a locally-sourced BGP route installed in IPv6 RIB.

  Workaround: Disable SNMP IPv6 polling.

- CSCua06629

  Symptoms: The **sh ipv6 mobile pmipv6 mag** global command does not show any output.

  Conditions: The symptom is observed only when domain and MAG configurations are present.

  Workaround: If MAG configuration is complete (all requisite access interfaces and peers are configured) then this issue will not be seen.

- CSCua07791

  Symptoms: A Cisco ISR G2 running Cisco IOS Release 15.2(2)T or later shows a memory leak in the CCSIP_SPI_CONTRO process.

  Conditions: The leak is apparent after 3-4 weeks. The process is CCSIP_SPI_CONTRO.

  Workaround: There is no workaround.

- CSCua07927

  Symptoms: MLDP traffic is dropped for local receivers on a bud node.

  Conditions: This issue is seen on doing stateful switchover (SSO) on bud node.

  Workaround: Using the **clear ip mroute vrf** *vrf name* ***** command for the effected VRFs will resume the MLDP traffic.

- CSCua13418

  Symptoms: RP-Announce packets are being replicated across all the tunnel interfaces and the count of replication is equal to the number of tunnel interfaces. For example, if there are 3 tunnel interfaces, then each tunnel should forward 1 RP-Announce packet each minute (with the default timer configured). However, in this case, each tunnel is forwarding 3 RP-Announce packets across each tunnel interface. This issue is not specific to the number of interfaces. It can happen with any number of tunnel interfaces.

  Conditions: This symptom is observed when filter-autorp is configured with the **ip multicast boundary** command. This issue is seen on the Cisco 3725 router too, where the incoming packets are being replicated because of the **filter-autorp** command.

  Workaround: Removing filter-autorp resolves the issue. However, you need to remove the **pim** and **boundary** commands first and then reapply the pim and boundary list without the **filter-autorp** keyword. Also, doing this might lead to redesigning of the topology to meet specific requirements.

  int Tun X no ip pim sparse-dense mode no ip multicast boundary XXXXXX filter-autorp

  int TuX ip pim sparse-dense mode ip multicast boundary XXXXXX

- CSCua13561

  Symptoms: After upgrading to Cisco IOS Release 15.2(2)S, users cannot get IP address via PPP IPCP from DHCP pool on a Cisco ASR router. There was no configuration change.

  Conditions: This symptom occurs when upgrading to Cisco IOS Release 15.2(2)S.

  Workaround: Remove the **vpdn authen-before-forward** command.

- CSCua14594

  Symptoms: Memory leak is seen when polling for the following PW MIBS:

  ```
  1.3.6.1.4.1.9.10.106.1.5.1.1 (cpwVcPerfTotalInHCPackets)
  1.3.6.1.4.1.9.10.106.1.5.1.2 (cpwVcPerfTotalInHCBytes)
  1.3.6.1.4.1.9.10.106.1.5.1.3 (cpwVcPerfTotalOutHCPackets)
  1.3.6.1.4.1.9.10.106.1.5.1.4 (cpwVcPerfTotalOutHCBytes)

  Address    Size   Alloc_pc  PID  Alloc-Proc       Name
  34417B84      308 13774B30  473  SNMP ENGINE     AToM VC event trace
  ```

  This memory leak, on repeated polling, may lead to device crash.

  Conditions: This symptom is observed with Cisco IOS Release 3.6S upon polling of the SNMP VC statistics query.

  Workaround: There is no workaround.

- CSCua15292

  Symptoms: Router may report unexpected exception with overnight stress traffic.

  Conditions: The symptom is observed with the following conditions:

  - Cisco ISR 3925E is deployed as DMVPN hub router and about 100Mbps traffic is controlled by PfR MC with dynamic PBR.
  - Router logs with

  ```
  %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
  destaddr=172.8.9.8, prot=50, spi=0xE8FB045F(3908764767), srcaddr=10.0.100.1, input
  interface=GigabitEthernet0/0
  ```

  Workaround: There is no workaround.

- CSCua16492

  Symptoms: Some IPv6 multi-hop BFD over BGP sessions flap.

  Conditions: Occurs on port-channel interfaces running IPv6 multi-hop BFD over BGP sessions after you perform an SSO.

  Workaround: There is no workaround.

- CSCua19425

  Symptoms: RP crashes at the far end, pointing to Watchdog Process BGP.

  Conditions: This symptom is observed when doing an FP reload at the near end. This issue is seen with EBGP sessions with BFD configured between near end and far end routers.

  Workaround: There is no workaround.

- CSCua21166

  Symptoms: Unable to form IPSec tunnels due to the following error:

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

  Conditions: Even though the router does not have 225 IPsec SA pairs, error will prevent IPSec from forming. Existing IPSec SAs will not be affected.

  Workaround: Reboot to clear out the leaked counter, or install hsec9 which will disable CERM (Crypto Export Restrictions Manager).

  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 2.8/2.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:M/C:N/I:N/A:P/E:U/RL:W/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCua25943

  Symptoms: CPU Hog is observed on the LC when the number of IPv6 prefixes pumped in is more than 10,000.

  Conditions: This symptom is observed when more than 10,000 IPv6 prefixes are pumped into the router.

  Workaround: There is no workaround.

- CSCua26487

  Symptoms: SNMP loops at OID 1.3.6.1.4.1.9.9.645.1.2.1.1.1, and as a result, SNMP walk fails.

Conditions: This symptom is observed only on the SNMP getbulk request on 1.3.6.1.4.1.9.9.645.1.2.1.1.1.

Workaround: Exclude the MIB table from SNMP walk using SNMP view. See the below configurations.

```
snmp-server view <view name> iso included
snmp-server view <view name> ceeSubInterfaceTable excluded
snmp-server community <community> view <view name>nterfaceTable excluded
snmp-server community <community> view <view name>
```

- CSCua27852

  Symptoms: Traffic loss is seen in pure BGP NSR peering environment.

  Conditions: The symptom is seen on a Cisco router that is running Cisco IOS Release 15.2(2)S, and the BGP peerings to CEs and RR are all NSR enabled.

  Workaround: Enable the **bgp graceful-restart** command for RR peering.

- CSCua28346

  Symptoms: A router crashes during second rekey.

  Conditions: This symptom occurs with IKEv2 with RSA authentication.

  Workaround: There is no workaround.

- CSCua30053

  Symptoms: Authentication is failing for clients after some time because the radius_send_pkt fails, because it complains about the low IOMEM condition.

  Conditions: In AAA, minimum IO memory must be 512KB to process the new request. If the memory is less than this, AAA does not process the new authentication request. This is AAA application threshold. This application barriers are not valid in dynamic memory case. Such conditions are removed for NG3K platform.

  Workaround: There is no workaround.

- CSCua31794

  Symptoms: After reload with the debug image, framed E1 lines are down.

  Conditions: On checking the “show controller SONET”, the default controller framing mode is taken as “crc4”. However before reload the configuration for those E1s were configured as “no-crc4”. Customer configured them on the E1s as “no-crc4” and it started working fine and the “show controller SONET” framing output changed to “no-crc4”. As per running configuration still the configuration is not showing “no-crc4”, as it should show as the default is CRC4. So the current issue is configuring “no-crc4”, it is not showing in running configuration and not saved and after reload it shows again CRC4 and services go down again.

  Workaround: Configure E1s as “no-crc4” and they would be working fine, but such changes are not being saved in configuration, so if reload reoccurs all these services go down again.

- CSCua31903

  Symptoms: IPv6 traffic is forwarded to wrong VRF when address is the same on both VRFs.

  Conditions: This symptom is observed in an IPv6 MPLS VPN network that has PE routers, which have multiple CE routers connected. The CE routers are in different IPv6 VRFs. The CE routers have the same IPv6 address. The PE routers are dual and use dual stack. The problem happens on a 6VPE setup when the CEs share same the IP address.

  Workaround: There is no workaround.

- CSCua33287

  Symptoms: ES+: L2TPv3 entries are programmed incorrectly after restart.

  Conditions: This symptom is observed when some L2TPv3 sessions are established on ES+ module. After the restart of ES+, some np entries may not program correctly. As the result, ES+ will stop to transmit packets.

  This condition will recover after executing **shut/no shut** on physical interfaces.

  Workaround: There is no workaround.

- CSCua33527

  Symptoms: Traceback seen after second or third switchover:

  ```
  %LFD-SW2-3-SMBADEVENT: Unexpected event CO_WAIT_TIMEOUT for state RUNNING -Traceback=
  7908E9Cz 7909848z 79099CCz 7909B9Cz 78DBF20z 523292Cz 522C1D4z
  ```

  Conditions: The symptom is observed with a quad-sup scenario/setup. This traceback is seen on the new active RP after second switchover onwards.

  Workaround: There is no workaround.

- CSCua33821

  Symptoms: CPU utilization shoots up to 99% after configuring crypto maps.

  Conditions: The symptom is observed after applying crypto maps.

  Workaround: There is no workaround.

- CSCua34033

  Symptoms: A Cisco ME 3800X hangs after boot.

  Conditions: It is possible for an evaluation scaled license to be configured on the router and scaled services license configured. EULA acceptance can be ignored when configuring this. When the Cisco ME 3800X is rebooted, the router needs to program itself differently for a scaled license than a base license, but it cannot do so without the EULA being accepted so the router issues a prompt on the console port. The router will wait here until a user has responded. However, if a user is not on the console port to see this EULA message, they will not know that it is waiting for an EULA response. The router will continue to wait.

  This is not seen on purchased licenses as they are not installed unless the EULA is accepted.

  Workaround: When using evaluation licenses, accept the EULA upon configuring a license on the router or only reload the router from a connection to the console port after configuring the router to use an evaluation license.

- CSCua34638

  Symptoms: A crash is seen on RP2, when the **show platform software shell command package** command is issued.

  Conditions: This symptom is observed when the **show platform software shell command package** command is issued. It impacts the RP2 (x86_64_*) image only.

  Workaround: There is no workaround. Do not issue the **show platform software shell command package** command.

- CSCua35235

  Symptoms: Trace route for TP does not work as expected.

  Conditions: This symptom occurs with a TP setup.

  Workaround: There is no workaround.

- CSCua37898

  Symptoms: Memory leaks are observed with @crypto_ss_enable_ipsec_profile on VSS.

  Conditions: The memory leaks are seen when OSPFv3 authentication is enabled over virtual link, and the OSPFv3 process is restarted.

  Workaround: There is no workaround.

- CSCua38881

  Symptoms: Router reloads at clear_dspm_counter_per_bay.

  Conditions: This issue is observed from Cisco IOS interim Release 15.2(3.16)M0.1 on Cisco 5350 and Cisco 5400 routers.

  Workaround: There is no workaround.

- CSCua39107

  Symptoms: In a FlexVPN Spoke to Spoke setup, Resolution reply goes via the Tunnel interface to the Hub.

  Conditions: This symptom is only observed when NHO is added for the V-Access, overriding an existing route. This issue is not seen when H route is added.

  Workaround: Distribute the summarized address from the Hub, thus avoiding addition of NHO at the Spokes. The Spokes will then add H route instead of NHO.

- CSCua40273

  Symptoms: The ASR1k crashes when displaying MPLS VPN MIB information.

  Conditions: Occurs on the ASR1K with version 15.1(02)S software.

  Workaround: Avoid changing the VRF while querying for MIB information.

- CSCua40369

  Symptoms: DMM timestamping is not happening for IFM over EVC Xconnect and OFM over port-channel.

  Conditions: DMM timestamping is not happening in the following conditions when:

  1. Interface is used as core interface in EVC Xconnect.
  2. Interface is used as a member in a port-channel.

  Workaround: There is no workaround.

- CSCua40790

  Symptoms: Memory leaks when SNMP polling cbgpPeer2Entry MIB.

  Conditions: This symptom occurs when BGPv4 neighbors are configured.

  Workaround: There is no workaround if this MIB is to be polled.

- CSCua41082

  Symptoms: In/op traffic drop is observed on endor 10 gig port in mixed mode.

  Conditions: This issue is seen after upgrading Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCua41398

  Symptoms: The SUP720 crashes.

  Conditions: Occurs when you issue the sh clns interface | i ^[A-Z]|Number of active command multiple times via script with following error and decodes:

```
%ALIGN-1-FATAL: Corrupted program counter 00:53:22 EET Tue Jun 5 2012
pc=0x0 , ra=0x411514F4 , sp=0x55A8B080

c7600s72033_rp-adventerprisek9-m.122-33.SRE5.symbols.gz read in
Enter hex value: 0x407F5B70 0x407F612C 0x407E026C 0x42BCA588 0x407EDDFC
0x41A78BB8 0x41A78B9C
0x407F5B70:get_alt_mode(0x407f5b68)+0x8
0x407F612C:get_mode_depth(0x407f6118)+0x14
0x407E026C:parse_cmd(0x407ded18)+0x1554
0x42BCA588:parser_entry(0x42bca360)+0x228
0x407EDDFC:exec(0x407ed344)+0xab8
0x41A78BB8:r4k_process_dispatch(0x41a78b9c)+0x1c
0x41A78B9C:r4k_process_dispatch(0x41a78b9c)+0x0
```

Workaround: There is no workaround.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

  Conditions: The issue is seen on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua45114

  Symptoms: Default sessions will not establish when you apply VRF as a service to the default policy. VRF can only be applied to a default session by assigning a VRF on the access-interface. However with dedicated sessions, one cannot apply a VRF on the access-interface and VRF transfer at the same time. If we require VRF transfer on dedicated sessions, we need VRF transfer on lite sessions as well.

  Conditions: This symptom is seen when access-side interface is in the default VRF. VRF is applied as a service to the default policy.

  Workaround: There is no workaround.

- CSCua45122

  Symptoms: Multicast even log preallocated memory space needs to be conserved on the low-end platform.

  Conditions: This symptom is observed with multicast even log.

  Workaround: There is no workaround.

- CSCua45548

  Symptoms: Router crashes with **show ip sla summary** on longevity testing.

  Conditions: The symptom is observed with Cisco 2900, 1900, and 3945 routers configured with IPSLA operations. The router which was idle for one day crashes on issuing the command **show ip sla summary**.

  Workaround: There is no workaround.

- CSCua47570

  Symptoms: The **show ospfv3 event** command can crash the router.

  Conditions: The symptom is observed when “ipv4 address family” is configured and redistribution into OSPFv3 from other routing protocols is configured.

Workaround: Do not use the **show ospfv3 event** command.

- CSCua48584

  Symptoms: The Cisco ME 3600X's ARP resolution may fail after flexlink switchover.

  Conditions: This symptom is observed on the Cisco ME 3600X running Cisco IOS Release 15.2(S) or Cisco IOS Release 15.2(2)S1 with flexlink configured.

  Workaround: Shut the active port of the flexlink pair. In other words, do a manual switchover through CLI.

- CSCua48807

  Symptoms: Complete traffic loss is observed.

  Conditions: This symptom is observed when queue-limit and default WRED "random-detect" are configured in a class and dynamically modify queue- limit of that class.

  Workaround: There is no workaround.

- CSCua51991

  Symptoms: An invalid SPI message is seen throughout the lifetime of IPsec SA.

  Conditions: This symptom is observed with SVTI-SVTI with a GRE IPv6 configuration. When bringing up 1K sessions, an invalid SPI is seen. There is also inconsistency between the number of child SAs in IKEv2 and the number of IPsec SAs on the same box.

  Workaround: There is no workaround.

- CSCua52289

  Symptoms: CPU hog is seen on the line card due to Const2 IPv6 process.

  Conditions: This symptom occurs with 4 core facing tunnels. Upon FRR cutover, the CPU hog is observed.

  Workaround: There is no workaround.

- CSCua52977

  Symptoms: DHCPv6 solicitations are sent over the air. This should be filtered, as it is normally client->network and not a flood type of traffic.

  Conditions: This symptom applies to any network with clients using IPv6.

  Workaround: There is no workaround.

- CSCua53772

  Symptoms: Router crashes when scheduling a y1731 DMM IP SLA probe to run.

  Conditions: This symptom happens when the probe's target cfm mep is configured under service instance with double tag encapsulation.

  Workaround: There is no workaround.

- CSCua55539

  Symptoms: CE devices ping is failing on SAToP/CESoPSN.

  Conditions: This issue is observed only with ECMP at the core.

  Workaround: There is no workaround.

- CSCua55691

  Symptoms: A Cisco IOS memory leak is observed.

  Conditions: This symptom is seen when unconfiguring/reconfiguring BGP AD VFIs.

Workaround: There is no workaround.

Further Problem Description: This issue is seen during longevity run.

- CSCua56802

  Symptoms: QoS will not work on one of the subinterfaces/EVC.

  Conditions: This symptom occurs when HQoS policy is configured on more than one subinterface/EVC on ES+ and then add flat SG on them.

  Workaround: Remove and reapply SG.

- CSCua57728

  Symptoms: Traffic loss of ~25s is seen upon doing TE FRR Cutover with IPv6 prefixes.

  Conditions: This symptom is observed with four core facing tunnels, and 100,000 IPv6 prefixes. Shut the primary interface and check for the traffic loss.

  Workaround: There is no workaround.

- CSCua58100

  Symptoms: The syslog is flooded with the following traceback message:

  ```
  %SYS-2-NOTQ: unqueue didn't find 7F3D26BDCCD8 in queue
  7F3CA5E4A240 -Process= "RADIUS Proxy", ipl= 0, pid= 223
  -Traceback= 1#e0ee0ce60492fdd11f0b03e0f09dc812  :400000+873623 :400000+2547652
  :400000+20F9217 :400000+6C70C9C :400000+6C69C71 :400000+6C682BC :400000+6C68183
  ```

  Conditions: Occurs under the following conditions:

  - You establish 36k EAPSIM sessions using a RADIUS client on server A.
  - You establish 36k roaming sessions using a RADIUS client on server B.
  - The roaming sessions have the same caller-station-id but use a different IP address than the EAPSIM sessions.

  Workaround: There is no workaround.

- CSCua60395

  Symptoms: When an IPv6 packet is received via EoMPLS pseudowire, the packet is punted to the CPU and sent back on the pseudowire.

  Conditions: This has been identified on a Cisco ME3600X with Cisco IOS Release 15.2(1)S1.

  Workaround:

  Option 1: Configure the xconnect under a interface vlan and configure a (dummy) IP address. Example:

  interface vlan XXX

  ip address A.B.C.D M.M.M.M

  xconnect N.N.NN <vc-id> encapsulation mpls

  Option 2: Block IPv6 packets on remote end so that these packets are not sent over pseudowire.

- CSCua64546

  Symptoms: In a scaled setup with IPV4 and IPV6 ACL together (not necessarily on the same interface), IPV4 ACLs may stop working if the IPV6 ACL configured later overwrites the IPv4 ACL results and vice versa.

  Conditions: This symptom is observed with IPV4 and IPV6 ACLs configured on the box.

Workaround: There is no perfect workaround. Reconfiguring the IPV4 ACL can recover the functionality but will affect the IPV6 ACL.

Further Problem Description: Only the IPV4 or IPV6 ACL configuration will work.

- CSCua64700

  Symptoms: The IPsec tunnel state goes to Up-Idle after 4-5 days of the router being up and running.

  Conditions: This symptom is observed if you have low rekey value, as with the rekey, the new SPI gets allocated. This issue is seen with WS-IPSEC-3 and to verify this, check the below counter.

  ```
  show crypto ace spi
  ```

  If there is no decrement in the SPI allocated counter and there is a consistent increment in the counter, the chances are high that you will encounter this issue.

  Once the value reaches 61439, you will encounter this issue.

  ```
  MTCVPNK03#sh cry ace spi
  SPI in use ......................... 0
  Normal SPI allocated ................ 61439
  ```

  Workaround: There is no workaround. You need to reload the box.

- CSCua67532

  Symptoms: IPsec sessions fail to come up.

  Conditions: This symptom occurs when Site-Site crypto configuration using crypto map is applied on SVI, and when no ISAKMP profile is configured under that crypto map.

  Workaround: There is no workaround.

- CSCua67795

  Symptoms: The router does not transmit Y.1731 Delay Measurement Message (DMM) values using QinQ encapsulation.

  Conditions: Occurs with the following configuration:

  - An EFP is configured and applied to a bridge-domain.
  - The EFP is configured with QinQ encapsulation.
  - A Y.1731 Delay Measurement Message (DMM) value is applied.
  - The Y.1731 traffic uses a CoS value other than 0.

  Workaround: There is no workaround.

- CSCua67998

  Symptoms: System crashes.

  Conditions: This symptom occurs after adding or removing a policy-map to a scaled GRE tunnel configuration.

  Workaround: There is no workaround.

- CSCua68243

  Symptoms: IGMP and PIM control packets are not reaching RP. As a result, mac-address table for IGMP snooping entries is not populated.

  Conditions: This symptom can be seen on a Cisco 7600 series router that is running Cisco IOS where we have IGMP and PIM control packets coming in on an SVI only after the condition where the SVI link state went down and came up again. This does not affect routed ports.

  Workaround: Unconfigure and reconfigure the SVI.

- CSCua69657

  Symptoms: Traceback is seen when executing the **show clock detail** command.

  Conditions: This symptom is seen when executing the **show clock detail** command with Cisco IOS interim Release 15.3(0.4)T image.

  Workaround: There is no workaround.

- CSCua70065

  Symptoms: CUBE reloads on testing DO-EO secure video call over CUBE when SDP passthru is enabled.

  Conditions: The symptom is observed when running Cisco IOS interim Release 15.3(0.4)T.

  Workaround: There is no workaround.

- CSCua71038

  Symptoms: Router crash.

  Conditions: The symptom is observed with a Cisco router that is running Cisco IOS Release 15.2(3)T1. The router may crash during the failover test with OCSP and CRL configured.

  Workaround: Configure OCSP or CRL but not both

- CSCua72199

  Symptoms: Unsolicited RAs from the switch is forwarded as mcast RAs over the air to the wireless clients. It should be a unicast packet. CAPWAP packet header from the switch is populated with L2 MGID and not IPv6 RA MGID (L3) and forwarded as multicast over air.

  Conditions: This symptom is seen with Standalone Newton 48 with a couple of APs and a couple of wireless clients with IPv6 enabled. IPv6 unicast routing is enabled on the switch.

  Workaround: There is no workaround.

- CSCua72440

  Symptoms: The REP VLAN load balancing does not happen correctly when two REP edge no-neighbor ports are configured. Traffic does not flow as expected.

  Conditions: This symptom is seen with Cisco IOS Release 15.2(4)S image that is loaded on a Cisco 7600 box. Two REP edge no-neighbor ports along with VLAN Load balancing are configured. The correct VLANs are not blocked/opened on the respective ports.

  Workaround: There is no workaround.

- CSCua78782

  Symptoms: Authentication of EzVPN fails.

  Conditions: The symptom is observed with BR-->ISP-->HQ.

  Workaround: There is no workaround.

- CSCua80204

  Symptoms: EoMPLS remote port shutdown feature does not work.

  Conditions: This symptom is observed if xconnect and a service instance are configured under the same interface.

  Workaround: There is no workaround.

- CSCua83609

  Symptoms: With 10 VRFs, traffic is forwarded through data and default-mdt address. The PEs are connected in a serial fashion, and total number of PEs is over 200. After the number of PEs becomes more than 50, the CPU usage goes high as a result of both software and hardware switching of mVPN control packets like Data-MDT.

  Conditions: This issue has been seen under the following conditions:

  - Cisco ME 3600X is running Cisco IOS Release 15.2(4)S but is not release specific.
  - Multicast stream can be received on any type of interface (L2/L3).

  Traffic is stopped as the CPU hog/crash is seen. Issue can be verified via the following:

  "show processes cpu sorted | e 00"

  Workaround: There is no workaround.

- CSCua84879

  Symptoms: Crash at slaVideoOperationPrint_ios.

  Conditions: The symptom is observed when IPSLA video operations are configured and **show running-config** is issued.

  Workaround: There is no workaround.

- CSCua84923

  Symptoms: Following a misconfiguration on a two-level hierarchical policy with a user-defied queue-limit on a child policy, the UUT fails to attach the QoS policy on the interface even when corrected queueing features are used.

  Conditions: This symptom is observed with the following conditions:

  1. The issue must have the user-defined queue-limit defined.
  2. This error recovery defected is confirmed as a side effect with the c3pl cnh compoent project due to ppcp/cce infrastructure enhancement.

  Workaround: There is no workaround.

- CSCua85837

  Symptoms: Depending on the aces in the redirect-list ACL used, only a subnet of the traffic gets redirected based on ports.

  Conditions: This symptom is observed when the WCCP service has a redirect-list ACL applied which in turn has port-specific aces in them.

  Workaround: Remove the L4 operators from the redirect-list ACL.

- CSCua85934

  Symptoms: A session provisioning failure is seen in the ISG-SCE interface. The deactivate or disconnect request has the message authenticator wrongly calculated.

  Conditions: This symptom is observed with the ISG-SCE interface.

  Workaround: There is no workaround.

- CSCua86310

  Symptoms: When relay is configured with unnumbered interface, it appears the packet is sent out of the loopback interface (instead of the serial interface) to the server, which does not receive the packet.

Conditions: The issue happens only when unnumbered loopback address is used on the relay interface which connects to server. If an IPv6 address is used directly on the interface, it works fine.

Workaround: Use numbered interface instead of unnumbered interface.

- CSCua87944

  Symptoms: In an IPv6 snooping policy, the keyword “prefix-list” has no effect on control packet. The keyword only affects the binding table recovery. In an “ipv6 nd raguard” policy, the limited-broadcast keyword appears though it is deprecated. It should be hidden and is always on.

  Conditions: These symptoms are observed in an IPv6 snooping policy and IPv6 and RA-guard policy.

  Workaround: There is no workaround.

- CSCua88341

  Symptoms: Multicast traffic on P2P GRE tunnel will get dropped.

  Conditions: This symptom usually happens in scenarios like SSO, which is done after VRF deletion or addition. Here the P2P GRE tunnel will be in the VRF.

  Workaround: Do a shut/no shut of the P2P GRE tunnel interface.

- CSCua91104

  Symptoms: ISIS adjacency process shows traceback messaging related to managed timer.

  Conditions: This symptom is seen when configuring isis network point-to-point on LAN interface with isis bfd or isis ipv6 bfd enabled. The traceback does not happen always. It depends on timing.

  Workaround: Disable isis bfd or isis ipv6 bfd before issuing **isis network point-to-point** command. Restore isis bfd or isis ipv6 bfd configuration on LAN interface.

- CSCua93136

  Symptoms: The switch crashes when sending the DHCPv6 packet with “ipv6 snooping” on VLAN configurations.

  Conditions: This symptom occurs when sending the DHCPv6 packet with “ipv6 snooping” configured on VLAN configurations.

  Workaround: There is no workaround.

- CSCua94947

  Symptoms: RP crashes when downloading FreeRadius Framed-IPv6-Route on MLPPP sessions.

  Conditions: This symptom occurs when downloading radius Framed-IPv6-Route.

  Workaround: There is no workaround.

- CSCua98690

  Symptoms: The ES+/ES20/SIP-400 (any card which supports EVC) card may crash due to memory corruption.

  Conditions: This symptom is observed when the MAC ACL is configured on EFP.

  Workaround: There is no workaround.

- CSCua98902

  Symptoms: FIBIDB is not getting initialized.

  Conditions: This symptom is observed when LFA FRR is configured Cisco ME 3800X.

  Workaround: There is no workaround.

- CSCub07382

  Symptoms: NHRP cache entry for the spokes gets deleted on NHRP timer expiry even though there is traffic flowing through the spoke to spoke tunnel.

  Conditions: This symptom is seen with FlexVPN spoke to spoke setup.

  Workaround: Configure the same hold time on both tunnel interface and the virtual-template interface.

- CSCub07673

  Symptoms: IPsec session does not come up for spa-ipsec-2g if ws-ipsec3 is also present. “Volume rekey” is disabled on Zamboni.

  Conditions: This symptom occurs if we have “volume rekey” disabled on Zamboni.

  Workaround: Do not disable the volume rekey on Zamboni.

- CSCub09124

  Symptoms: MDT tunnel is down.

  Conditions: This symptom is seen in MVPN. If the **ip multicast boundary** command on non-current RPF interface blocks the MDT group, it may cause MDT tunnel failure.

  Workaround: Adding the **static join** command under PE loopback interface may work around the problem temporarily.

- CSCub10951

  Symptoms: At RR, for an inter-cluster BE case, there are missing updates.

  Conditions: This symptom is observed with the following conditions:

  1. The following configuration exists at all RRs that are fully meshed: - bgp additional-paths select best-external - nei x advertise best-external
  2. For example, RR5 is the UUT. At UUT, there is:

     - Overall best path via RR1.

     - Best-external (best-internal) path via PE6 (client of RR5): for example, the path is called “ic_path_rr5”.

     - Initially, RR5 advertises “ic_path_rr5” to its nonclient iBGP peers, that is, RR1 and RR3.
  3. At PE6, unconfigure the route so that RR5 no longer has any inter-cluster BE path. RR5 sends the withdrawals to RR1 and RR3 correctly.
  4. At PE6, reconfigure the route so that RR5 will have “ic_path_rr5” as its “best-external (internal) path”. At this point, even though the BGP table at RR5 gets updated correctly, it does not send the updates to RR1 and RR3. They never relearn the route.

  Workaround: Hard/soft clear.

- CSCub15542

  Symptoms: Configuring mpls lsp trace results in IOSD restart.

  Conditions: This symptom occurs when configuring mpls lsp trace results in IOSD restart.

  Workaround: There is no workaround.

- CSCub17985

  Symptoms: A memory leak is seen when IPv6 routes are applied on the per-user sessions.

  Conditions: This symptom is seen if IPv6 routes are downloaded as a part of the subscriber profile. On applying these routes to the sessions, a memory leak is observed.

Workaround: There is no workaround.

- CSCub18997

  Symptoms: A Cisco ME 3800 may crash after the following error message is displayed:

  ```
  %SYS-6-STACKLOW: Stack for process Non-Qos Events Process running low, 0/6000
  ```

  Conditions: This symptom is observed on a Cisco ME 3800 that is running Cisco IOS Release 15.2(2)S1.

  Workaround: There is no workaround.

- CSCub21468

  Symptoms: UDP header is corrupted randomly.

  Conditions: This symptom is observed with the Cisco 7609-S (RSP720-3C-GE) running Cisco IOS Release 12.2(33)SRE5, with the VRF Aware LI feature.

  Workaround: There is no workaround.

- CSCub24079

  Symptoms: TAR bundle does not get downloaded through the **archive** command.

  Conditions: This symptom applies to any conditions.

  Workaround: Untar externally and copy to flash/ucode1 directories.

- CSCub25360

  Symptoms: In a Flexlink switchover scenario, it seems that for some reason, the Cisco ME 3600X switch does not send out a dummy mcast packet for the SVI.

  Conditions: This symptom is observed with a Cisco ME 3600X Flexlink switchover.

  Workaround: There is no workaround.

- CSCub31592

  Symptoms: After the flap of the interface with EVC configured, the box is no longer adding second tag to the traffic. Forwarding is broken. See the following example:

  ```
  service instance 100 ethernet
    encapsulation dot1q 10
    bridge-domain 100
  ```

  Conditions: This symptom is seen with flap of the interface.

  Workaround: There is no workaround.

- CSCub31622

  Symptoms: RSTP BPDUs are not tunneled over xconnect.

  Conditions: This has been observed on Cisco IOS Releases 15.1(02)EY02a, 15.1(02)EY3 and 15.2(2)S1 with below configuration on the Cisco ME3800X:

  ```
  int gix/x
   service instance 100
    encapsulation default
    l2protocol tunnel
    bridge-domain 500

   int vlan 500
   platform rewrite imposition tag push 1 symmetric
  ```

```
xconnect x.x.x.x 500 encapsulation mpls
```

This may create STP inconsistency and blocked VLANs on CE side.

Workaround: There is no workaround.

- CSCub31902

  Symptoms: Alignment correction tracebacks are seen from within the diag_dump_lc_l2_table() cosmetic issue, which create temporary memory inconsistencies in the function.

  Conditions: This symptom occurs in normal conditions, during bootup time, provided testMacNotification fails.

  Workaround: Disable bootup diagnostics or disable the testMacNotification health monitoring test.

- CSCub32500

  Symptoms: Router crashes in EIGRP due to chunk corruption.

  Conditions: This symptom is seen on EIGRP flaps.

  Workaround: There is no workaround.

- CSCub33877

  Symptoms: During the “issue loadversion” where we are downgrading from Texel (or later) to Yap (v151_1_sg_throttle or earlier), the standby RP keeps reloading due to the out of the sync of configuration.

  Conditions: The issue occurs during ISSU loadversion operation. The newer version of image supports the IPv6 multicast while the older version of image does not.

  Workaround: There is no workaround.

- CSCub35388

  Symptoms: The **port-channel min-links** command is rejected under port-channel.

  Conditions: This symptom is seen when port-channel has vrf configuration.

  Workaround: first configure min-link command and then configure vrf command under port-channel

- CSCub36217

  Symptoms: When the Cisco ME 3800 router is running Cisco IOS Release15.2(4)S software, if EVC maximum MAC security address limit is reached for a service instance, new MAC address is not rejected.

  Conditions: This symptom is observed when EVC MAC security is enabled under a service instance.

  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 1.7/1.3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:L/AC:L/Au:S/C:N/I:P/A:N/E:U/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

- CSCub42920

  Symptoms: KS rejects rekey ACK from GM with message (from “debug crypto gdoi ks rekey all”):

  ```
  GDOI:KS REKEY:ERR:(get:0):Hash comparison for rekey ack failed.
  ```

  The keys and policies in the rekey packet are correctly installed by the GM, but the rekey ACK does not get processed by the KS. This leads to rekey retransmissions, GM re-registration and potential disruption of communication.

Conditions: Rekey ACK validation in Cisco IOS Releases 15.2(4)M1 (ISR-G2) and 15.2(4)S/XE 3.7S (Cisco ASR1000) is incompatible with other software releases.

A KS that runs Cisco IOS Releases 15.2(4)M1 or 15.2(4)S/XE 3.7S will only be able to perform successful unicast rekeys with a GM that runs one of those two versions. Likewise, a KS that runs another version will only interoperate with a GM that also runs another version.

Workaround: Use multicast rekeys.

- CSCub46570

  Symptoms: The image cannot be built with an undefined symbol.

  Conditions: This symptom occurs as the commit error triggers the compiling issue.

  Workaround: There is no workaround.

- CSCub47520

  Symptoms: “Match dscp default” matches router initiated ARP packets.

  Conditions: This issue is seen on Cisco 7600 ES+ line cards.

  Workaround: Classify router generated packets using source mac address using a MAC ACL.

- CSCub48262

  Symptoms: Router crashes in ROMMON.

  Conditions: This symptom occurs with RSP processor.

  Workaround: There is no workaround.

- CSCub49291

  Symptoms: Static tunnels between hubs and spokes fail to rebuild.

  Conditions: This symptom occurs when reloading hub on the DMVPN IPv6 setup with DPD on-demand enabled on all spokes.

  Workaround: There is no workaround.

- CSCub54872

  Symptoms: A /32 prefix applied to an interface (e.g. a loopback) is not being treated as connected. This can then prevent Half-Duplex VRFs from operating correctly.

  Conditions: This symptom is seen when the prefix applied to an interface is for a host route (/32 for IPv4 or /128 for IPv6).

  Workaround: Use a shorter prefix.

- CSCub62897

  Symptoms: SVI is not coming up for a long time even though there are active ports in that VLAN.

  Conditions: This issue happens with flexlink + preemption + VLAN load balance configuration.

  Workaround: There is no workaround.

- CSCub67101

  Symptoms: The POS interface line protocol is down with encapsulation PPP in an MPLS setup.

  Conditions: This symptom occurs when configuring encapsulation PPP on both ends of PE1 and CE1, and then configuring xconnect in the customer-facing interface of PE1.

  Workaround: Reconfigure the xconnect settings. Then, the interface will come up in the proper state.

- CSCub73159

  Symptoms: IOSD crash is observed.

Conditions: This symptom is seen when bringing up 8k PPP sessions with QoS and eBGP routes.

Workaround: There is no workaround.

- CSCub73430

  Symptoms: A Cisco router that is running Cisco IOS Release 15.2.(4)S ipBaseK9 feature set crashes when an interface that a QoS policy attached to it comes up.

  Conditions: This symptom occurs on a Cisco router that is running Cisco IOS Release 15.2.(4)S ipBaseK9 feature set.

  Workaround: Use other feature sets.

- CSCub78830

  Symptoms: Traffic matching WCCP service gets black-holed.

  Conditions: This symptom is seen in vrf-wccp scenario and on redirection into MPLS cloud.

  Workaround: There is no workaround.

- CSCub78917

  Symptoms: PIM VRF neighbor is not coming up.

  Conditions: This symptom is seen with MVPN v6 configurations.

  Workaround: Use an earlier image where it was proper.

- CSCub79102

  Symptoms: Router crashes with MVPNV6 setup.

  Conditions: This symptom is seen while unconfiguring VRF. The router crashes.

  Workaround: There is no workaround.

- CSCub92588

  Symptoms: The chopper SPA does not come up.

  Conditions: This symptom is seen when the router reloads.

  Workaround: There is no workaround.

- CSCub98588

  Symptoms: The IPsec session does not comes up for spa-ipsec-2g if you have “volume rekey” disabled.

  Conditions: This symptom is seen if we have “volume rekey” disabled on spa-ipsec-2g.

  Workaround: Do not disable the volume rekey on spa-ipsec-2g.

- CSCub99756

  Symptoms: A Cisco ASR 1000 router that is running Cisco IOS Release 15.2(4)S acting as a GM in a GETVPN deployment starts using the most recent IPSEC SA upon KS rekey instead of using the old key up to 30 seconds of expiration.

  Conditions: This symptom is observed only in Cisco IOS Release 15.2.(4)S.

  Workaround: There is no workaround.

- CSCuc08298

  Symptoms: ISSU between XE 3.7S base version (Cisco IOS Release 15.2(4)S) and Cisco IOS Release 15.2(4)S2 or later releases may not pass in the presence of trifecta modules.

  Conditions: This issue is specific to setups with trifecta modules.

Workaround: In order to make ISSU work with (Cisco IOS Release 15.2(4)S) base release, power down the trifecta module using **no power enable mod** t*rifecta slot(s)* and then carry out the ISSU procedure to releases later than Cisco IOS Release 15.2(04)S2.

- CSCuc11090

  Symptoms: With Cisco ME3600/ME3800 as the encap box in MVPN, if the packet size if greater than the default MTU, packets will not flow out of the box.

  Conditions: This symptom is seen with MVPN configured on Cisco ME3600/ME3800 box. The box should be a core encap box and traffic should be going on the tunnel to hit this situation. Only packets beyond the default MTU will not go out and get dropped.

  Workaround: Send packets of smaller size from the source so that after encaping with the 24 bytes of outer IP of the MDT tunnel does not go beyond the size of egressing interface MTU.

- CSCuc13364

  Symptoms: Egress service policy on EFP is dropping all traffic in egress. Offered rate equals drop rate. Interface output rate is zero, output drop is increasing.

  Conditions: This issue has been observed with Cisco ME36xx that is running Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCuc14023

  Symptoms: Cisco IOS build failure is due to signature verification.

  Conditions: This symptom is seen with Cisco 7600 build, RSP and SUP image.

  Workaround: There is no workaround.

- CSCuc15548

  Symptoms: Subscriber session on LAC/LNS is stuck in attempting state with “vpdn authen-before-forward” CLI configured and auto-service in the radius-profile.

  Conditions: The key to the issue is CLI “vpdn authen-before-forward” and one auto-service in the user profile in radius.

  Workaround: Configure and apply one policy-map with SESSION-START rule with at least one action.

- CSCuc15656

  Symptoms: REP occasionally fails when a peer device that is running REP on the same segment is reloaded.

  Conditions: This issue is seen when a remote device is reloaded. The REP state machines on both devices can get stuck.

  Workaround: Flap the link of the unit that did not go into the REP wait state. This will bring the REP statemachines at both ends.

Open Caveats—Cisco IOS Release 15.2(4)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.2(4)S. All the caveats listed in this section are open in Cisco IOS Release 15.2(4)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtl86057

  Symptoms: The loading of the standby RP and bulk sync times have increased on the XE3 throttle. Increases in time of up to 20-30% have been seen.

  Conditions: Under higher scale this problem becomes more noticeable.

  Workaround: There is non known workaround at this time. We are still investigating the problem.

- CSCtq24011

  Symptoms: Routers act like if local-proxy-arp is configured and does a proxy-arp even for the systems in the same subnet.

  Conditions: The router receives arp request on an interface while the interface is not fully initialized. The connected routes are not added in the routing table yet. This causes proxy-arp reply and wrong arp entry stuck forever.

  Workaround: **shut/no shut** on victim and offender routers.

- CSCtq56659

  Symptoms: Wrong LC programming with CEM interface.

  Conditions: Issue is seen after the initial configuration of HSPWs.

  Workaround: Soft OIR.

- CSCtr45030

  Symptoms: The SNMP timers process causes the router to exit global configuration mode or prevents the console from entering global configuration mode.

```
c7609#conf t
```

  Configuration mode is locked by process “319” user “unknown” from terminal “0”. Please try later.

```
c7609#show proc | in 319

  319 Mwe  9735348          928      21701      42 4412/6000   0 SNMP Timers
```

  Or

```
  c7609(config)#logging console
```

  Config session is locked by process “307”, user will be pushed back to exec mode. Command execution is locked, Please try later.

```
  c7609(config)#^Z
```

  Conditions: Occurs when you copy and paste large configurations, particularly a large number of VLAN configurations. The issue occurs without any SNMP configurations present.

  Workaround:

  - Option 1 - Disable RMON
  - Option 2 - If configuration is huge. Paste in multiple blocks.

  - Option 3 - Enable debug snmp timers. Paste the required configuration when the timer callbacks have finished executing.

- CSCtr94565

  Symptoms: Sp hung after the router crashes.

  Conditions: Occurs with bgp-pic core and enabled.

  Workaround: Disable the bgp pic.

- CSCts04802

  Symptoms: During vrf transfer, old services are removed but the new service is not applied.

  Conditions: This symptom is observed during a vrf transfer from v1 to v2.

  Workaround: There is no workaround.

- CSCts11715

  Symptoms: After shutting the tunnel, ISAKMP does not turn OFF.

  Conditions: This symptom is observed in a scaled DMVPN setup with more than 1k spokes.

  Workaround: There is no workaround.

- CSCts54641

  Symptoms: Various small/medium/big/VB chunks leak at the following functions:

  __be_snmp_decode_varbind

  __be_snmp_decode_sync_msg

  __be_k_ciscoFlashDeviceEntry_get

  __be_snmp_decode_varbind

  __be_mib_tlv_to_oid

  __be_mib_tlv_to_octet

  __be_snmp_decode_varbind

  Conditions: MIBs are being polled or SSO is done.

  Workaround: There is no workaround.

- CSCtw94737

  Symptoms: Standby supervisor keeps getting power-cycled due to RF request:

  ```
  %OIR-SP-3-PWRCYCLE: Card in module 6, is being power-cycled (RF request)
  ```

  Conditions: Symptom is observed during RPR downgrade from Cisco IOS 15S to Cisco IOS Release 12.2SRE.

  Workaround: Perform downgrade through reload.

- CSCtx15799

  Symptoms: An MTP on a Cisco ASR router sends an “ORC ACK” message through CRC for the channel ID that is just received but does not reply to the ORC for the next channel.

  Conditions: The symptom is observed when there is a very short time lapse between the ORC and CRC, say 1 msec.

  Workaround: There is no workaround.

- CSCtx23593

  Symptoms: Some virtual circuit (VC) information is missing in the Simple Network Management Protocol (SNMP) MIB object cAal5VccEntry from the output of the **snmpwalk** router configuration command. For example, The ATM VCs 4/0.120 exist on the router but are missing in the MIB.

  Conditions: This symptom is observed on a Cisco 7204VXR (NPE-G2) router that is running Cisco IOS Release 12.2(33)SRE5 (c7200p-advipservicesk9-mz.122-33.SRE5.bin) image in customer network. The symptom may also occur in other releases.

  Workaround:

  - Enter the **show atm vc** privileged EXEC command on the same device to obtain a complete list of all the VCs. Or,
  - Do the SNMPWALK suffixing the ifIndex of the interface to get the value. $ snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.2.1.2.2.1.2 | grep "4/0.120" IF-MIB::ifDescr.253 = STRING: ATM4/0.120-atm subif IF-MIB::ifDescr.254 = STRING: ATM4/0.120-aal5 layer

```
$ snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.2.1.2.2.1.2 | grep "4/0.120"

IF-MIB::ifDescr.253 = STRING: ATM4/0.120-atm subif

IF-MIB::ifDescr.254 = STRING: ATM4/0.120-aal5 layer


$  snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.4.1.9.9.66.1.1.1.1.3 | grep
9.9.66.1.1.1.1.3.254 ===> Got no entry of ifindex here in complete snmpwalk

$

$ snmpwalk -v 2c -c fwwrcmn na-salerno-ar011 .1.3.6.1.4.1.9.9.66.1.1.1.1.3.254
===> When done the SNMPWALK suffixing the ifindex, then getting the value which
can be one workaround.

SNMPv2-SMI::enterprises.9.9.66.1.1.1.1.3.254.200.106 = Counter32: 403633041
```

- CSCtx54882

  Symptoms: A Cisco router may crash due to bus error crash at voip_rtp_is_media_service_pak.

  Conditions: This symptom is been observed on a Cisco router that is running Cisco IOS Release 15.1(4)M2.

  Workaround: There is no known workaround.

- CSCtx59669

  Symptoms: Spikes are observed in UDP jitter RTT values for MPLS VPN based operations.

  Conditions: On a Cisco 7600 when there are a large number of packets configured per UDP operation, some packets (~1%) exhibit large RTT delays. This is especially noticeable when BGP is exchanging large number of routes.

  Workaround: There is no workaround.

- CSCtx72906

  Symptoms: Standby gets stuck in cold-bulk state and it does not come up in SSO mode even after few hours.

  Conditions: This symptom is seen with scale QoS configs applied on EVCs/subifs (L2VPN/L3VPN) and scale crypto configs.

  Workaround: There is no workaround.

- CSCty09682

  Symptoms: REP Primary edge fails to take part in REP.

  Conditions: Occurs on reload.

  Workaround: Flap the interface, and it will converge.

- CSCty10693

  Symptoms: Device crashes with what looks like a memory corruption.

  Conditions: Are not known at this time and will update as we have more information.

  Workaround: There is no workaround.

- CSCty22117

  Symptoms: When swapping ip addresses on an ethernet connection between an MWR2941 and a Cisco 7600. OSPF fails to re-establish.

  Conditions: Changing the IP address in the Cisco MWR2900 to the neighbors IP address and then changing the neighbors IP address to what was on the MWR causes the MWR to see a duplicate IP address and never allows the svi to participate in OSPF.

  Tested changing the IP address in the other equipment first and this works fine. Only when the Cisco MWR2900 is changed first do we see this issue.

  Workaround: “Change” the MWR address back to bad address:

  - This causes duplicate address. OSPF timers again expire.
  - Now change back the MWR address to final IP address. We will not have the duplicate address this time, and the OSPF process completes to FULL.

- CSCty31982

  Symptoms: Portchannel is in suspended state, with peer throwing messages that lacp is not enabled on remote node.

  Conditions: This symptom occurs on reload.

  Workaround: Remove/Add untagged service instance which would have l2peer stp,lacp configured.

- CSCty33037

  Symptoms: Out of memory is seen on sender

  Conditions: This symptom is observed on three Telepresence sessions running at the same time for maximum duration (10 minutes).

  Workaround: There is no workaround. Reduce duration or session number.

- CSCty47447

  Symptoms: IPv6 traffic over IPv6 sVTI tunnels gets dropped.

  Conditions: This symptom is seen under the following conditions:

  - Have GRE+IPsec tunnels configured with QoS.
  - Have IPv4 sVTI tunnels configured with QoS.
  - Have IPv6 sVTI tunnels configured.

  With all the above tunnels configured, traffic should flow on all the IPv4 IPsec and VTI tunnels and traffic rate should oversubscribe the QoS policy on them.

  Workaround: There is now workaround.

- CSCty53054

  Symptoms: Tracebacks show up on standby sometimes when **shut/unshut** of the p2mp TE tunnel.

  Conditions: This symptom is seen when a dual RP box **shut/noshut** of the p2mp TE tunnel may generate traceback. There is no functionality impact.

  Workaround: There is no workaround.

- CSCty57137

  Symptoms: SIP SPAs go out of service state in scaled subinterface config (more than 2000 subinterfaces on single GigE port).

  Conditions: While performing ISSU between iso1-rp2 and iso2-rp2 xe3.6 throttle image, after issu runversion, the SIP SPAs go out of service state. Need heavily scaled config. Seen when there are 2000 to 3000 subinterfaces on the single SPA and following limits are exceeded. Overall dual stack VRFs per box: 2800 dual stack limit on interface: 1000.

  Workaround: The issue is not seen in the following scenario:

  1. Before doing a load version from RP0 (initial active), issue the following command: asr1000# show ipv6 route table | inc IPv6.
  2. Note down the number of ipv6 route tables in the system.
  3. Do a load version.
  4. Wait for standby to come up to Standby hot.
  5. Enable standby console from RP0 (active) asr1000#configure terminal Enter configuration commands, one per line. End with CNTL/Z. asr1000(config)# asr1000(config)#redundancy asr1000(config-red)#main-cpu asr1000(config-r-mc)#standby console enable.
  6. Login to standby console and issue the following command asr1000-stby# show ipv6 route table | inc IPv6 Again note down the number of IPv6 route tables in standby. If it is less than the number noted at step2, wait for some time and re-verify till it reaches the number noted in step 2.
  7. Issue issu runversion from RP0 (active)

- CSCty59891

  Symptoms: On the node where **shut/no shut** is issued, traffic does not reach IPsec VSPA which is supposed to get encrypted.

  Conditions: Issue **shut/no shut** on the GRE tunnel protected with IPsec and QoS configured on this IPsec Tunnel.

  Workaround: Remove and attach “tunnel protection ipsec profile”.

- CSCty64216

  Symptoms: On unconfiguring a scaled ACL, a router crash is noted.

  Conditions: This symptom is seen with an ACL having 1000 ACEs or more when unconfigured.

  Workaround: There is no workaround.

- CSCtz06740

  Symptoms: MPLS LSP ping does not work when PE-to-PE TE tunnel is down.

  Conditions: PE-to-PE tunnel is down, and Next hop to PE1 has TE tunnel to remote PE2. PE1 is Cisco ME3600.

  Workaround: There is no workaround.

- CSCtz17175

  Symptoms: Traffic loss for 100 seconds will be seen.

  Condition: When the router with ~32K VCs configured is reloaded.

  Workaround: There is no workaround.

- CSCtz37164

  Symptoms: The requests to the radius server are retransmitted even though the session no longer exists. This causes unnecessary traffic to radius and also radius gets requests for an invalid session.

  Conditions: This issue occurs when the radius server is unreachable and the CPE times out the session

  Workaround: The issue can be seen as per the conditions mentioned above. This can be avoided by making sure that the radius server is always reachable

- CSCtz49200

  Symptoms: OSPF IPv6 control packets are not encrypted/decrypted.

  Conditions: Occurs while configuring the ipv6 ospf authentication.

  Workaround: There is no workaround.

- CSCtz50204

  Symptoms: Crash is seen while applying “vrf ivrf2” on Server.

  Conditions: Crash is seen while applying “vrf ivrf2” on Server.

  Workaround: There is no workaround.

- CSCtz50537

  Symptoms: Deactivation of ipv4 unicast rpf via radius does not work.

  Conditions: Occurs when you configure a user profile in Radius with an AVPair: Cisco-AVPair += “lcp:interface-config=no ip verify unicast source reachable-via rx”.

  No error appears in debugs or logs. The same configuration works in Cisco IOS XE Release 2.x releases but does not work in 3.x releases.

  Workaround: There is no workaround.

- CSCtz62857

  Symptoms: RP crashes with segmentation fault pointing to IP RIB Update process.

  Conditions: This problem is seen if you issue the configuration command: no router bgp during the period between when BGP is first configured and when it completes routing protocol initialization and bulk sync to the standby.

  Workaround: Wait for BGP initialization and bulk sync to complete before issuing “no router bgp”. How long this takes will vary by platform, configuration, and routing table size. On an Cisco ASR 1004 with an RP2 route processor and a typical configuration and routing table size, this takes no longer than 20 minutes.

- CSCtz63438

  Symptoms: In a GETVPN environment, the group member continuously registers to keyserver.

  Conditions: The symptom is observed when the onboard crypto engine is disabled on a Cisco 1900 series platform.

  Workaround: There is no workaround.

- CSCtz69517

  Symptoms: IPv6 VRF data packets are getting punted to CPU.

  Workaround: There is no workaround.

- CSCtz70207

  Symptoms: The device experiences an I/O memory leak in the “Big” buffer pool.

  Conditions: Occurs when you configure NetFlow data export and the device is actively exporting traffic to a collector.

  Workaround: Disable NF/NF data export.

- CSCtz71084

  Symptoms: When prefix from CE is lost, the related route that was advertised as best-external to RR by PE0 does not get withdrawn.

  Conditions:

  PE0#conf t

  Enter configuration commands, one per line. End with CNTL/Z.

  PE0(config)#router bgp 1

  PE0(config-router)#address-family ipv4 vrf CE2

  PE0(config-router-af)#import path selection all

  PE0(config-router-af)#bgp recursion host

  PE0(config-router-af)#bgp advertise-best-external

  PE0(config-router-af)#end

  Even though the configs have SOO, it is not necessary for the repro.

  However, the issue is not happening if we shut the interface between PE0-CE2 from either side. Instead, need to do something like the following to stop CE2 to advertise the prefixes:

  CE2#conf t

  Enter configuration commands, one per line. End with CNTL/Z.

  CE2(config)#router bgp 2

  CE2(config-router)#no network 100.1.1.0 mask 255.255.255.0

  CE2(config-router)#no network 110.1.1.0 mask 255.255.255.0

  CE2(config-router)#no network 120.1.1.0 mask 255.255.255.0

  CE2(config-router)#

  Workaround: There is no workaround.

- CSCtz87622

  Symptoms: MLDP traffic is dropped for sometime (few min) couple of times after SSO.

  Conditions: Issue is seen soon after performing SSO.

  Workaround: There is no workaround.

- CSCtz90328

  Symptoms: Multicast traffic stops for some time because of CPU Hog on removal of the QoS policy-map from the service instance.

Conditions: Occurs when the Multicast traffic is bursty and is oversubscribing the queue.

Workaround: There is no workaround.

- CSCtz91502

  Symptoms: Nile unicast met shows multiple ReplicationContextQueueEntry, and traffic is flooded to all ports in vlan.

  Conditions: The issue is seen when a access port is in the same vlan as the rep segment. A rep flap is seen.

  Workaround: Clear mac-address table fixes the CQE entries.

- CSCtz92606

  Symptoms: MFR memberlinks - T1 serial intfs created under a CHOC12 controller, do not get decoupled from MFR even after the MFR bundle intf is deleted. And once the MFR bundle interface is reconfigured, the memberlinks does not appear under it.

  Conditions: MFR with memberlinks as T1 serials from CHOC12 sonet controller.

  Workaround: Unconfigure and reconfigure the “encap frame-relay MFRx” under each memberlink after reconfiguring the MFR bundle interface.

- CSCtz97297

  Symptoms: Router takes sporadically up to 5 seconds to forward multicast after IGMP join is received.

  Conditions: None.

  Workaround: Use static IGMP join on egress interface.

- CSCua01641

  Symptoms: The router’s NAS-IP address contained in the RADIUS Accounting-on packet is 0.0.0.0:

```
===
*May 17 14:34:22 JST: RADIUS:  Acct-Session-Id     [44]  10  "00000001"
*May 17 14:34:22 JST: RADIUS:  Acct-Status-Type    [40]  6   Accounting-On
        [7]
*May 17 14:34:22 JST: RADIUS:  NAS-IP-Address      [4]   6   0.0.0.0
         <<======Here!!!
*May 17 14:34:22 JST: RADIUS:  Acct-Delay-Time     [41]  6   0
===
```

  Conditions: Occurs when you restart the router.

  Workaround: There is no workaround.

- CSCua03201

  Symptoms: If the VPN ID of an existing Virtual Forwarding Interface (VFI) is changed on a dual-RP system, and then a stateful switchover (SSO) is performed, the new standby router may repeatedly reload.

  Conditions: This symptom has been observed in Cisco IOS Release 15.2(2)S/ Cisco IOS XE Release 3.6.0S and later.

  Workaround: In order to configure a new VPN ID for a VFI, completely remove the existing VFI and reconfigure it.

- CSCua06629

  Symptoms: The **sh ipv6 mobile pmipv6 mag globals** command does not show any output.

Conditions: The symptom is observed only when domain and MAG configurations are present.

Workaround: If MAG configuration is complete (all requisite access interfaces and peers are configured) then this issue will not be seen.

- CSCua07791

  Symptoms: ISR-G2 running Cisco IOS Release 15.2(2)T or later sees memory leak in CCSIP_SPI_CONTRO process.

  Conditions: The leak is apparent after 3-4 weeks. Process is CCSIP_SPI_CONTRO.

  Workaround: There is no workaround.

- CSCua07927

  Symptoms: MLDP Traffic is dropped for local receivers on a bud node.

  Conditions: Issue is seen on doing SSO (stateful switchover) on Bud node.

  Workaround: **clear ip mroute vrf** *vrf name** for the effected vrfs will resume the MLDP traffic.

- CSCua09764

  Symptoms: SSS Manager intermittently crashes when clearing sessions. This crash has been seen when issuing “clear subscriber session all” with a single L2 session and 600 default sessions.

  Conditions: This crash is difficult to reproduce and occurs more frequently when you have “debug subscriber policy all” enabled while continuously clearing sessions.

  Workaround: There is no workaround.

- CSCua13561

  Symptoms: After upgrading to Cisco IOS Release 15.2(2)S, users cannot get IP address via PPP IPCP from DHCP pool on Cisco ASR. There is no configuration change.

  Conditions: Upgrade from Cisco IOS Release 12.2(33) XNF2 to Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCua13804

  Symptoms: Router crashes when doing snmp query on ERM- Resource Groups.

  Condition: Crash occurs only when a resource group is configured.

  Work around: There is no workaround.

- CSCua20373

  Symptoms: After SSO, we will see all the GRE tunnels get admin down and it stays down until the security module SSC-600/WS-IPSEC-3 comes up. We see complete traffic loss during this time.

  Conditions: Have Vanilla GRE tunnels configured in the system where HA and IPsec Module SSC-600/WS-IPSEC-3 card is present and issue SSO.

  Workaround: There is no workaround.

- CSCua21238

  Symptoms: IOSD crashes at _ipv6_address_set_tentative.

  Conditions: Occurs while unconfiguring ipv6 subinterfaces.

  Workaround: There is no workaround.

- CSCua23451

  Symptoms: High convergence is seen on Cisco 7600 SUP720 switchover (oir or software cli) in 1 out of 10 readings.

Conditions: Occurs with high convergence on Cisco 7600 SUP720 switchover (oir or software cli) in 1 out of 10 readings.

Workaround: There is no workaround.

- CSCua23570

  Symptoms: IS-IS adjacency remains down on the standby RP while it is up on the active RP. If a switchover occurs this may result in an adjacency flap as the Standby transition to Active.

  Conditions: Occurs when you apply the multi-topology command under the IPv6 address family and the router receives IPv6 prefixes through IS-IS.

  Workaround: There is no workaround.

- CSCua24676

  Symptoms: VRF to global packet's length are corrupted by -1.

  Conditions: Issue is seen when the next-hop in vrf is global and recursive going out labled. Issue is seen from Cisco IOS Release 15.0(1)S3a onwards and not seen on Cisco IOS Release 15.0(1)S2.

  Workaround: Use next hop interface ip instead of recursive next hop.

- CSCua25943

  Symptoms: CPU Hog is seen on the LC with CMFI Background process hogging the CPU.

  Conditions: It is observed when more than 10k IPv6 prefixes are pumped into the router.

  Workaround: There is no workaround.

- CSCua26064

  Symptoms: IPv6 routes in the global routing table take up different adjacency entries.

  Conditions: It is seen when there are 4 core facing tunnels that load balance traffic to these prefixes. "show mls cef ipv6 <prefix> detail" shows the different adjacencies taken by different prefixes.

  Workaround: Have a single tunnel on the core facing side, instead of a load balanced path.

- CSCua26981

  Symptoms: A Cisco ASR router may crash due to a CPU Watchdog upon invocation of "show ip eigrp neighbor detail."

  ```
  CMD: 'sh ip eigrp nei detail'
  <snip>
  ASR1000-WATCHDOG: Process = Exec
  %SCHED-0-WATCHDOG: Scheduler running for a long time, more than the maximum configured
  (120) secs.
  -Traceback= ...
  ```

  Conditions: The Cisco ASR router must be experiencing rapid changes in EIGRP neighborship, such as during a flap. One way to artificially create this scenario is to mismatch the interface MTU.

  Workaround: There is no workaround.

- CSCua27842

  Symptoms: The Cisco ASR 1000 router crashes in Firewall code due to NULL l4_info pointer. Day 1 issue.

  Conditions: This symptom occurs when the Cisco ASR 1000 router acts as the MPLS L3VPN UHP. It crashes because FW/NAT requires the l4_info to be set. To trigger this issue, the following features must be configured:

  1. MPLS L3VPN (PE)

2. Zone Based FW/NAT
3. MPLS & MP-BGP loadbalance configured towards upstream router

Workaround: There is no workaround.

- CSCua27852

  Symptoms: Traffic loss is seen in pure BGP nsr peering environment.

  Conditions: The symptom is seen on Cisco router with Cisco IOS Release 15.2(2)S, and the bgp peerings to CEs and RR are all NSR enabled.

  Workaround: Enable the bgp graceful-restart for RR peering.

- CSCua29001

  Symptoms: ANCP truncated line rate is not seen on standby and the policy application will differ from that on active.

  Conditions: Occurs when **ancp truncate** *value* CLI is enabled and port ups received on BRAS.

  Workaround: There is no workaround.

- CSCua30956

  Symptoms: Network is not reachable behind CEs when primary PW fails and secondary PW takes over.

  Conditions: Primary PW fails. Secondary takes over but network behind CEs are not reachable.

  Workaround: There is no workaround.

- CSCua30963

  Symptoms: DHCP client is not getting a response for DHCPREQUEST message.

  Conditions: DHCP server did not send an ACK to the DHCPREQUEST sent by the client.

  Workaround: There is no workaround.

- CSCua31794

  Symptoms: After reload with the debug image, framed E1 lines are down.

  Conditions: On checking the “show controller SONET”, the default controller framing mode is taken as “crc4”. However before reload the configuration for those E1s were configured as “no-crc4”. Customer configured them on the E1s as “no-crc4” and it started working fine and the “show controller SONET” framing output changed to “no-crc4”. As per running configuration still the configuration is not showing “no-crc4”, as it should show as the default is CRC4. So the current issue is configuring “No-crc4”, it is not showing in running configuration and not saved and after reload it shows again CRC4 and services go down again.

  Workaround: Configure E1s as “no-crc4” and they would be working fine, but such changes are not being saved in configuration, so if reload reoccurs all these services go down again.

- CSCua31934

  Symptoms: Crash seen at __be_address_is_unspecified.

  Conditions: The symptom is observed with the following conditions:

  1. It occurs one out of three times, and it is a timing issue.
  2. DMVPN tunnel setup between Cisco 2901 as spoke and Cisco ASR 1000 as hub.
  3. Pass IPv4 and IPv6 traffic between the hub and the spoke for 5-10 minutes.
  4. It can occur with v6 traffic alone.

5. If you remove the tunnel interface on the ASR and add it again using **conf replace nvram:startup-config** the crash will occur.

Workaround: Use CLI to change configuration instead of the rollback feature.

- CSCua33287

  Symptoms: ES+: L2TPv3 entries are programmed incorrectly after restart.

  Conditions: This symptom is observed when some L2TPv3 sessions are established on ES+ module. After the restart of ES+, some np entries may not program correctly. As the result, ES+ will stop to transmit packets.

  This condition will recover after executing **shut/no shut** on physical interfaces.

  Workaround: There is no workaround.

- CSCua33527

  Symptoms: Traceback seen after second or third switchover:

  ```
  %LFD-SW2-3-SMBADEVENT: Unexpected event CO_WAIT_TIMEOUT for state RUNNING -Traceback=
  7908E9Cz 7909848z 79099CCz 7909B9Cz 78DBF20z 523292Cz 522C1D4z
  ```

  Conditions: The symptom is observed with a quad-sup scenario/setup. This traceback is seen on the new active RP after second switchover onwards.

  Workaround: There is no workaround.

- CSCua34033

  Symptoms: Cisco ME 3800x hangs after boot.

  Conditions: It is possible for an Evaluation Scaled license to be configured on the router and scaled services license configured. EULA acceptance can be ignored when configuring this. When the Cisco ME 3800x is rebooted, the router needs to program itself differently for a scaled license than a base license but it cannot do so without the EULA being accepted so the router issues a prompt on the console port. The router will wait here until a user has responded. However, if a user is not on the console port to see this EULA message, they will not know that it is waiting for an EULA response and so the router will continue to wait.

  This is not seen on purchased licenses as they are not installed unless the EULA is accepted.

  Workaround: When using evaluation licenses, accept the EULA upon configuring a license on the router or only reload the router from a connection to the console port after configuring the router to use an evaluation license.

- CSCua37333

  Symptoms: The router displays an EIGRP Active Route in the routing table.

  Conditions: Occurs on the Cisco ASR 1000 with Cisco IOS Releases 15.1(3)S2 and 15.1(3)S3.

  Workaround: There is no workaround.

- CSCua40273

  Symptoms: The Cisco ASR1000 router crashes when displaying MPLS VPN MIB information.

  Conditions: Occurs on the ASR1000 router with Cisco IOS Release 15.1(2)S.

  Workaround: There is no workaround.

- CSCua41398

  Symptoms: The Cisco SUP720 crashes.

  Conditions: Occurs when you issue the sh clns interface | i ^[A-Z]|Number of active command multiple times via script with following error and decodes:

```
%ALIGN-1-FATAL: Corrupted program counter 00:53:22 EET Tue Jun 5 2012
pc=0x0 , ra=0x411514F4 , sp=0x55A8B080

c7600s72033_rp-adventerprisek9-m.122-33.SRE5.symbols.gz read in
Enter hex value: 0x407F5B70 0x407F612C 0x407E026C 0x42BCA588 0x407EDDFC
0x41A78BB8 0x41A78B9C
0x407F5B70:get_alt_mode(0x407f5b68)+0x8
0x407F612C:get_mode_depth(0x407f6118)+0x14
0x407E026C:parse_cmd(0x407ded18)+0x1554
0x42BCA588:parser_entry(0x42bca360)+0x228
0x407EDDFC:exec(0x407ed344)+0xab8
0x41A78BB8:r4k_process_dispatch(0x41a78b9c)+0x1c
0x41A78B9C:r4k_process_dispatch(0x41a78b9c)+0x0
```

Workaround: There is no workaround.

- CSCua42806

  Symptoms: A Cisco RSP720 crashes after a couple of hours traffic passing though MPLS L2VPN VC.

  Conditions: MPLS L2VPN VC setup, with the Cisco 7600 in the MPLS L3 path to the VC endpoints. This issue is seen after several hours of forwarding traffic.

  Workaround: The crash is not seen if the Cisco 7600 terminates the L2 VC.

- CSCua42860

  Symptoms: The standby SUP module displays an “in progress to standby cold-bulk” message and crashes.

  Conditions: Occurs when you an perform an archive configuration.

  Workaround: There is no workaround.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

  Conditions: The issue is seen on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua45114

  Symptoms: Default sessions will not establish when you apply VRF as a service to the default policy. VRF can only be applied to a default session by assigning a VRF on the access-interface. However with dedicated sessions, one cannot apply a VRF on the access-interface and VRF transfer at the same time. Thus if we require VRF transfer on dedicated sessions, we need VRF transfer on lite sessions as well.

  Conditions: Access-side interface is in the default VRF, VRF is applied as a service to the default policy.

  Workaround: There is no workaround.

- CSCua46210

  Symptoms: Packets are not decrypted for specific ezvpn client and ping fails.

  Conditions: Occurs while sending traffic, only first 50 ezvpn clients are reachable.

Workaround: There is no workaround.

- CSCua46304

  Symptoms: Crash is seen at __be_nhrp_group_tunnel_qos_apply.

  Conditions: Occurs when flapping a DMVPN tunnel on the hub in a scale scenario.

  Workaround: There is no workaround.

- CSCua48584

  Symptoms: Cisco ME3600X ARP resolution may fail after flexlink switchover

  Conditions: Occurs on Cisco ME3600X that is running Cisco IOS Releases 15.2S or 15.2(2)S1 with flexlink configured.

  Work around: Shut the active port of the flexlink pair, in other words do a manual switchover through CLI.

- CSCua48807

  Symptoms: Complete traffic loss is observed.

  Conditions: Occurs when having queue-limit and default WRED “random-detect” configured in a class and dynamically modify queue-limit of that class.

  Workaround: There is no workaround.

- CSCua49803

  Symptoms: Ingress PE in mvpnv6 setup crashes.

  Conditions: Issue is seen on performing SSO with mvpnv6 sm and ssm traffic for 50 vrfs.

  Workaround: There is no workaround.

- CSCua52289

  Symptoms: CPU Hog is seen on the LC, due to Const2 IPv6 process.

  Conditions: Have 4 core facing tunnels. Upon FRR cutover, observing hog.

  Workaround: There is no workaround.

- CSCua52439

  Symptoms: MLD reports are not received on ES+.

  Conditions: On sending MLD joins on ES+ the reports are not received on the router.

  Workaround: There is no workaround.

- CSCua57585

  Symptoms: CPU utilization increases with XE33 builds.

  Conditions: Occurs when a device forwards traffic on PPPoE connections.

  Workaround: There is no workaround.

- CSCua57728

  Symptoms: Observing traffic loss of ~25s upon doing TE FRR Cutover with IPv6 prefixes.

  Conditions: Have 4 core facing tunnels, 100k IPv6 prefixes. Shut the primary interface and check for the traffic loss.

  Workaround: There is no workaround.

- CSCua57883

  Symptoms: UDLD flaps are reported over the BR Interface when L2TP configuration is done over the 6500.

  Conditions: No known Trigger of the issue. But when this issue is seen it caused the MST to recalculate which eventually lead to the BFD to flap for ISIS and thus causing the network outage.

  Workaround: There is no workaround.

- CSCua58100

  Symptoms: The syslog is flooded with the following traceback message:

  ```
  %SYS-2-NOTQ: unqueue didn't find 7F3D26BDCCD8 in queue 7F3CA5E4A240 -Process= "RADIUS
  Proxy", ipl= 0, pid= 223
  -Traceback= 1#e0ee0ce60492fdd11f0b03e0f09dc812 :400000+873623 :400000+2547652
  :400000+20F9217 :400000+6C70C9C :400000+6C69C71 :400000+6C682BC :400000+6C68183
  ```

  Conditions: Occurs under the following conditions:

  - You establish 36k EAPSIM sessions using a RADIUS client on server A.
  - You establish 36k roaming sessions using a RADIUS client on server B.
  - The roaming sessions have the same caller-station-id but use a different IP address than the EAPSIM sessions.

  Workaround: There is no workaround.

- CSCua60395

  Symptoms: When a IPv6 packet is received via EoMPLS pseudowire, the packet is punted to the CPU and sent pack on the pseudowire.

  Conditions: This has been identified on a Cisco ME3600x with Cisco IOS Release 15.2(1)S1.

  Workaround:

  Option 1: Configure the xconnect under a interface vlan and configure a (dummy) IP address. Example: interface vlan XXX ip address A.B.C.D M.M.M.M xconnect N.N.NN <vc-id> encapsulation mpls

  Option 2: Block IPv6 packets on remote end, so that these packets are not send over pseudowire.

- CSCua61201

  Symptoms: Unexpected reload with BFD configured is seen.

  Conditions: Occurs when a device is configured with BFD it may experience unexpected reloads.

  Workaround: There is no workaround.

- CSCua61814

  Symptoms: Overhead accounting configuration is changed on XE37 image.

  Conditions:

  XE34: overhead accounting configure at parent only

  XE35: overhead accounting configure at parent only

  XE37: overhead accounting need to be configured on both parent and child policy

  Workaround: There is no workaround.

- CSCua63182

  Symptoms: Incorrect minimum bandwidth is displayed when a 0k received.

  Conditions: Different behavior in Cisco ASR code when Min BW of 0 Kbit is received.

```
2.6.2 uses 10 Gbps as Min BW in case Min BW = 0 received
3.4.3 uses 1 Kbit as Min BW in case Min BW = 0 received
```

Workaround: There is no workaround.

- CSCua64546

  Symptoms: In scaled setup with IPV4 and IPV6 ACL together (not necessarily on same interface), IPV4 ACLs may stop working if IPV6 ACL configured later overwrites the ipv4 acl results and vice versa.

  Conditions: Occurs when IPV4 and IPV6 ACLs are configured on the box.

  Workaround: Not perfect workaround, reconfiguring the IPV4 ACL can recover the functionality but will affect the IPV6 ACL.

  Further Problem Description: Only IPV4 or IPV6 ACL configuration will work.

- CSCua64676

  Symptoms: MVPNv4 traffic is not flowing properly from remote PE to UUT.

  Conditions: With Agilent traffic on, after removal/addition of MDT configs for the MVRFs configured on the UUT, MVPNv4 traffic is not flowing properly from remote PE to UUT.

  Workaround: There is no workaround.

- CSCua64700

  Symptoms: IPSec Tunnel States goes to Up-Idle after 4-5 days of router up and running.

  Conditions: If you have low rekey value, the chances of hitting this issue is high, as with the rekey the new spi gets allocated. Seen with WS-IPSEC-3 and to verify this, check the below counter show crypto ace spi.

  If no decrement in spi allocated counter and there the consistent increment in counter, the chances are high, you will hit this issue.

  Once the value reaches to 61439, you will hit this issue.

  ```
  MTCVPNK03#sh cry ace spi
  SPI in use ........................... 0
  Normal SPI allocated ................. 61439
  ```

  Workaround: There is no workaround.

- CSCua76281

  Symptoms: Crash of RSP720-3C-GE @ vc_qos_change is seen.

  Conditions: Device crashes unexpectedly. Last function processed was vc_qos_change.

  Workaround: There is no workaround.

- CSCua80204

  Symptoms: **service instance 1 ethernet myevc** command is not accepted

  Conditions: Occurs if the interface is already attached with xconnect.

  Workaround: There is no workaround.

- CSCua81608

  Symptoms:

  While running 4RURP1 ISSU sub package forwarding run with all feature from XE352/XE36->latest mcp_dev,iosd crashes and router reloads again and again in final ISSU upgrade.

Conditions: Occurs when applying the running config attached in the ddts. Perform an ISSU. Router crashes.

Workaround: There is no workaround.

- CSCua81998

  Symptoms: Doing ISSU RV in Cisco 7600 box with ES40 LC may sometimes cause crash in ES40 LC.

  Conditions: ISSU RV XE3.7 or XE3.8 to XE3.6.1

  Workaround: There is no workaround.

- CSCua84147

  Symptoms: Router crashes during “sh run | format” CLI execution

  Conditions: This crash is seen only during “sh run | format” execution. All other CLI executions are fine.

  Workaround: Avoid executing “sh run | format”. Instead “sh run” can be executed.

- CSCua84860

  Symptoms: The device cannot ping a device in a separate VRF.

  Conditions: Occurs when the device is configured as an ISG subscriber and is in a different VRF than the target IP address.

  Workaround: Configure an ACL that permits the IP address range and configure the log keyword.

- CSCua85239

  Symptoms: Flapping BGP sessions are seen with change route-map after/before mpls-ip or mtu be configured:

  ```
  *Jun  3 18:20:20.792 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to
  2.2.2.5(17744) tableid - 0

  *Jun  3 18:20:30.488 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to
  2.2.2.5(17744) tableid - 0

  *Jun  3 18:20:36.451 UTC: %BGP-5-ADJCHANGE: neighbor 6.6.6.5 Down BGP Notification
  sent

  *Jun  3 18:20:36.451 UTC: %BGP-3-NOTIFICATION: sent to neighbor 6.6.6.5 4/0 (hold time
  expired) 0 bytes

  *Jun  3 18:20:36.569 UTC: %BGP_SESSION-5-ADJCHANGE: neighbor 6.6.6.5 VPNv4 Unicast
  topology base removed from session  BGP Notification sent

  *Jun  3 18:20:40.184 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to
  2.2.2.5(17744) tableid - 0

  *Jun  3 18:20:44.619 UTC: %BGP-5-ADJCHANGE: neighbor 6.6.6.5 Up

  *Jun  3 18:20:49.926 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to
  2.2.2.5(17744) tableid - 0

  *Jun  3 18:20:59.604 UTC: %TCP-6-BADAUTH: Invalid MD5 digest from 6.6.6.5(179) to
  2.2.2.5(17744) tableid - 0
  ```

  Conditions: The issue is seen between two BGP peers with matching MD5 passwords configured and can be triggered by:

  1. Removing and re-adding “route-map” with “mpls-ip” configuration for the BGP peering on one side of the peering.

     ```
     conf t

     router bgp A
     ```

```
address-family vpnv4
(no) neighbor x.x.x.x route-map SET-MED out
(no) neighbor y.y.y.y route-map SET-MED out

conf t
interface GigabitEthernet1/2/2
(no) mtu 2000
```

or

2. Removing and re-adding “route-map” with “mtu” configuration for the BGP peering on one side of the peering.

```
conf t
router bgp A
address-family vpnv4
(no) neighbor x.x.x.x route-map SET-MED out
(no) neighbor y.y.y.y route-map SET-MED out

conf t
interface GigabitEthernet1/2/2
(no) mpls ip
```

3. Peering Down and MD5 error do not always occur. Only happens one or two times within 100 tested of (1) and (2).

Workaround: There is no workaround.

- CSCua88341

  Symptoms: Multicast traffic on P2P GRE tunnel will get dropped.

  Conditions: It usually happens in scenarios like SSO is done after vrf del/add. Here the P2P GRE tunnel will be in the VRF.

  Workaround: **shut/no shut** of the P2P GRE tunnel interface.

- CSCua91473

  Symptoms: crypto_kmi_add_data_to_pyld memory leak is seen at IPSEC key engine process.

  Conditions: IPSEC key engine holding memory keeps increasing.

  Workaround: There is no workaround.

- CSCua92557

  Symptoms: The active FTP data channel sourced from the outside may not work as expected. Other protocol inspections that expect pinhole or door for connections initiated from the outside may be affected as well.

  Conditions: This symptom was first identified on the Cisco ASR router running Cisco IOS Release 15.1(3)S3 with VASI+VRF+PAT+FW. This issue is seen when the FTP client is on the inside and the active FTP server is on the outside.

  Workaround: Static NAT will work.

- CSCua94947

  Symptoms: RP crashes when downloading Freeradius Framed-IPv6-Route on MLPPP sessions.

  Conditions: Occurs when downloading radius Framed-IPv6-Route.

  Workaround: There is no workaround.

- CSCua98690

  Symptoms: ES+ Card may crash due to memory corruption.

  Conditions: Occurs when MAC ACL is configured on EFP.

  Workaround: There is no workaround.

- CSCub01238

  Symptoms: Hardware appeared to be incorrectly programmed on ES card.

  Conditions: TE tunnel with FRR.

  Workaround: Once the control plane and data plane get out of sync, the only way to resolve is to tear down the tunnel's LSP.

- CSCub02618

  Symptoms: Cisco 7600 router configured with VFI with RSP720 processor may crash with memory related issues.

  Conditions: Multiple Config/unconfig and SSO.

  Workaround: There is no workaround.

- CSCub02709

  Symptoms: Router crash indicates memory allocation failure.

  Conditions: Occurs when loading router bgp process config with scaled ipv4 and ipv6 address-family neighbors.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(4)S

All the caveats listed in this section are resolved in Cisco IOS Release 15.2(4)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCej11786

  Symptoms: A Cisco 2600 router reloads when a clear counter is performed on the router. This crash is reproducible only after making a number of calls first.

  Conditions: This symptom has been observed on a Cisco 2600 router.

  Workaround: There is no workaround.

- CSCtj93356

  Symptoms: Batch suspending from platform causes the MFIB on line card to go into reloading state.

  Conditions: This symptom occurs when MFIB on line card goes into reloading state and then finally to purge state after removal/addition of MVRFs is done followed by a line card reset.

  Workaround: There is no workaround.

- CSCtl01184

  Symptoms: Sometimes an EVC that is configured on ES+ sends frames out with CFI bit set in the VLAN tag.

  Conditions: This symptom is observed on EVCs that are configured on ES+.

  Workaround: There is no workaround.

- CSCtl18571

  Symptoms: On a Cisco 7600 series router with etherchannels configured, the **show etherchannel load-balance module** *x* command shows VLAN included even though the excluded VLAN has been configured globally using the **port-channel load-balance** *algorithm* **exclude vlan** command.

  Conditions: This symptom occurs when the system is operating in pfc3c or pfc3cxl mode with CFC and DFC card without per module load-balance.

  Workaround: This is an issue with the **show** command. The algorithm itself is not affected. The load-balancing algorithm is applied correctly as configured globally.

- CSCtr36083

  Symptoms: IKE SAs are not cleared. Ping fails over the IPsec tunnel.

  Conditions: This symptom occurs when SAs are cleared by using the **clear crypto session local** *address* command.

  Workaround: There is no workaround.

- CSCtr93412

  Symptoms: Crash seen on mwheel process.

  Conditions: The symptom is observed with GETVPN multicast followed by **clear crypto gdo**.

  Workaround: There is no workaround.

- CSCts00341

  Symptoms: When executing a CLI that requires domain-name lookup such as **ntp server** *server.domain.com*, the command fails with the following message on the console:

```
ASR1k(config)#ntp server server.domain.com         <<<    DNS is not resolved
with dual RPs on ASR1k
Translating "server.domain.com "...domain server (10.1.1.1) [OK]

%ERROR: Standby doesn't support this command              ^
% Invalid input detected at '^' marker.

ASR1k(config)#do sh run | i ntp
ASR1k(config)#
```

  Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

  Workaround: Instead of using *hostname* in the command, specify the IP address of the host.

- CSCts12499

  Symptoms: SPA firmware crash at one bay leads to SPA crash in another bay.

  Conditions: This symptom is observed when “test crash cema” is executed from the SPA console. leading to the SPA in the other bay to reload. Also, the crashinfo is not present in the RP disk.

  Workaround: There is no workaround.

- CSCts44393

  Symptoms: A Cisco ASR 1000 crashes.

  Conditions: The symptom is more likely to occur when a large number of VRFs are repeatedly configured and deleted.

  Workaround: There is no workaround.

- CSCts68626

  Symptoms: PPPoE discovery packets causes packet drop.

  Conditions: The symptom is observed when you bring up a PPPoE session and then clear the session.

  Workaround: There is no workaround.

- CSCtt26692

  Symptoms: Router crashes due to memory corruption. In the crashinfo you may see:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk xxxxxxx data
  xxxxxxxx chunkmagic xxxxxxxx chunk_freemagic EF4321CD -
  Process= "CCSIP_SPI_CONTROL", ipl= 0, pid= 374
  chunk_diagnose, code = 1
  chunk name is MallocLite
  ```

  Conditions: Router is configured for SIP. When a translation-rule is configured to translate a number to one with more digits, the router may crash when the translation takes effect, such as when a call is forwarded.

  Workaround: Configuring “no memory lite” configurations can be used as a workaround in some cases (depending on the length of the phone numbers), but will cause the router to use more memory. If the translation-profile is configured to translate forwarded calls, then avoid or disable the option to forward the call.

- CSCtt35379

  Symptoms: BGP Processing Enhancements.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt70133

  Symptoms: The RP resets with FlexVPN configuration.

  Conditions: This symptom is observed when using the **clear crypto session** command on the console.

  Workaround: There is no workaround.

- CSCtt94440

  Symptoms: The Cisco ASR 1000 series router RP may reload.

  Conditions: This symptom is observed when an etoken is in use and the **show crypto eli all** command is issued.

Workaround: Avoid using the **show crypto eli all** command. However, you can use the **show crypto eli** command.

- CSCtu01601

  Symptoms: A Cisco ASR1000 series router may crash while executing the **write memory** command.

  Conditions: This issue may be triggered when the memory in the router is low.

  Workaround: There is no workaround.

- CSCtu14409

  Symptoms: The “Insufficient bandwidth 2015 kbps for bandwidth guarantee” error message is displayed when configuring a policy map with “priority level xxx” and then updating it with “police cir xxx”.

  Conditions: This symptom occurs when the priority is configured without a specific rate. This issue is only seen with a Cisco ASR 1000 series router.

  Workaround: Configure police before priority.

- CSCtu23195

  Symptoms: SNMP ifIndex for serial interfaces (PA -4T/8T) becomes inactive after PA OIR.

  Conditions: The symptom is observed with a PA OIR.

  Workaround: Unconfigure and reconfigure the channel-groups of the controller and reload the router.

- CSCtu40028

  Symptoms: The SCHED process crashes.

  Conditions: The issue occurs after initiating TFTP copy.

  Workaround: There is no workaround.

- CSCtu43120

  Symptoms: Service accounting start is not sent for L2TP sessions.

  Conditions: This symptom is observed with L2TP.

  Workaround: There is no workaround.

- CSCtv28434

  Symptoms: GDOI cannot start negative GM re-register timer and prints out traceback at func crypto_gdoi_start_re_register_timer().

  Conditions: The symptom is observed with both IP (v4/v6) GDOI crypto maps configured on the dual-stack interface and GMs re-registration triggered.

  Workaround: Do not trigger GMs to re-register.

- CSCtv36812

  Symptoms: Incorrect crashInfo file name is displayed during crash.

  Conditions: The symptom is observed whenever a crash occurs.

  Workaround: There is no workaround.

- CSCtw46229

  Symptoms: Small buffer leak. The PPP LCP configuration requests are not freed.

  Conditions: The symptom is observed with PPP negotiations and the session involving PPPoA.

Workaround: Ensure all your PPP connections stay stable.

- CSCtw50952

  Symptoms: A Cisco ASR series router crashes due to memory exhaustion after issuing the **clear ip ospf**. This symptom was not observed before issuing this command.

```
ACC-CDC-NET-Pri#sh mem stat
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)
Largest(b)
 Processor   30097008   1740862372   279628560   1461233812   1460477804
 1453167736
 lsmpi_io   97DD61D0     6295088     6294120         968         968
   968
```

  Conditions: This symptom is observed upon executing the **clear ip ospf** causing tunnel interfaces to flap.

  Workaround: There is no workaround.

- CSCtw53121

  Symptoms: ES+ goes into major state occasionally on reload or SSO.

  Conditions: This issue is seen in the Cisco 7600 router with 40 gig ES+ line card that is running Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCtw55401

  Symptoms: The SPA-1XCHSTM1/OC3 card goes to out of service after SSO followed by OIR.

  Conditions: This issue is seen with the SPA-1XCHSTM1/OC3 card with Cisco 7600- SIP-200 combination.

  Workaround: There is no workaround.

- CSCtw55424

  Symptoms: SSH with “vrf” in command line for IPv6 addr/host is not working. For example: **ssh -l** *username* **-vrf** *vrfname ipv6 add/host*.

  Conditions: The symptom is observed when **ip ssh source-interface** is not defined and the user specifies the VRF by command line (e.g.: **ssh -l** *username* **-vrf** *vrfname ipv6 add/host*).

  Workaround: Use **ip ssh source-interface** *interface-name* and connect with **ssh -l** *username (IPv4/IPv6)(addr/host)*.

- CSCtw62310

  Symptoms: The **cells** keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service- policy”.

  Conditions: The symptom is observed when removing the policy-map from map-class.

  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw70298

  Symptoms: A router crashes after the router boots up with scaled configuration and L2/L3 Distributed EtherChannel (DEC) or port-channel.

  Conditions: This symptom occurs only if there are more than two or more DFCs (ES+ and other equivalents) and with L2/L3 DEC configured such that one of the DFCs takes much longer to come up than the other.

  Workaround: There is no workaround.

- CSCtw73530

  Symptoms: Unable to delete metadata sessions.

  Conditions: This symptom is observed when more than 100 metadata sessions are created.

  Workaround: Disable metadata and then enable it. Note that this will remove all the flows.

- CSCtw79171

  Symptoms: Platform asserts at adjmgr_l2_create.

  Conditions: This symptom occurs with excessive flapping of a link.

  Workaround: There is no workaround.

- CSCtx05726

  Symptoms: When creating a bulk number of traffic engineering tunnel interfaces on the router with option **tunnel mpls traffic-eng exp-bundle master**, the standby route processor crashes.

  Conditions: This symptom is seen with a specific set of configurations which has creation of a large number of tunnel interfaces (scale number 1000) followed by creation of large number of master tunnels (scale number 1000). Copying such a configuration to the router causes this crash on the standby processor.

  The tunnel interfaces which are created at the beginning of the configuration are added as members to the master tunnels in the later part of the configuration. During this phase of creation of the master tunnels and adding member tunnels, these tunnel interfaces go through a cycle of "create-delete-create". When such a configuration is being synced to the standby route processor along with the resulting create-delete events, the standby processor crashes.

  This point where crash happens is random and can happen during configuration of any of the master tunnels.

  Workaround: There is no workaround. Once the standby reboots after the crash, the configurations on the active are synced to the standby and this sync does not cause any crash. Crash is only during the initial copy of the configurations to the router.

- CSCtx06813

  Symptoms: Installation fails, "rwid type l2ckt" error messages appear, and the VC may fail to come up on Quad-Sup router only. Though this error may appear for multiple other reasons, this bug is specific to Cisco Catalyst 6000 Quad-Sup SSO only.

  Conditions: The symptom is observed in a scaled scenario, doing second switchover on Quad-Sup router.

  Workaround: There is no workaround.

- CSCtx11598

  Symptoms: A router reload causes a Cisco Shared Port Adapter (SPA) failure with the following error message:

  ```
  % CWAN_SPA-3-FAILURE: SPA-2CHT3-CE-ATM[2/2]: SPA failure
  ```

This failure can cause the SPA to go to one of the following states:

- none
- standby reset
- down

This failure leads to unexpected system reload.

Conditions: This symptom is observed during router reload for 15-20 times.

Workaround: Ensure that all of the library shared objects are loaded at the time of the SPA initialization.

- CSCtx32527

  Symptoms: The **show crypto session** command reveals the flexVPN GRE tunnel is in a DOWN state instead of DOWN-negotiating.

  Conditions: The symptom is observed with “ip address negotiated” configured on the GRE tunnel interface (with tunnel protection). The tunnel is unable to reach the gateway initially.

  Workaround: Configure an IP address on the tunnel interface instead of “ip address negotiated”.

- CSCtx35064

  Symptoms: Traffic remains on blackholed path until holddown timer expires for PfR monitored traffic class. Unreachables are seen on path, but no reroute occurs until holddown expires.

  Conditions: This symptom is seen under the following conditions:

  - MC reroutes traffic-class out a particular path (BR/external interface) due to OOP condition on the primary path.
  - Shortly after enforcement occurs, an impairment on the new primary path occurs causing blackhole.
  - PfR MC does not declare OOP on the new primary path and attempt to find a new path until Holddown timer expires. Causes traffic loss.

  Workaround: Reduce the holddown timer to 90 seconds (minimum value) to minimize impact.

- CSCtx36095

  Symptoms: A traceback is seen after applying DMLP configurations while doing a line card reload.

  Conditions: This symptom occurs during a line card reload.

  Workaround: There is no workaround.

- CSCtx38121

  Symptoms: IPv6 traffic is not passing through the interface attached with service policy matching IPv6 traffic using IPv6 ACL.

  Conditions: This symptom is observed when attaching a service policy matching IPv6 traffic that is configured using ipv6 access-list on EFP of an interface, which will lead to a traffic drop.

  Workaround: There is no workaround.

- CSCtx47213

  Symptoms: The following symptoms are observed:

  1. Session flap when iBGP local-as is being used on RRs.
  2. Replace-as knob is not working in iBGP local-as case.

Conditions:

1. The session will flap when iBGP local-as is used on the RR client and RR sends an update.
2. Replace-as knob even used is ignored and prefixes are appended with local-as.

Workaround: Do not use iBGP local-as.

- CSCtx57073

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

  ```
  "Segmentation fault(11), Process = Metadata HA"
  ```

  Conditions: This symptom is observed while upgrading the router from Cisco IOS XE Release 3.6 to mcp dev.

  Workaround: The required changes have been made with this DDTS to prevent the crash.

- CSCtx62138

  Symptoms: Standby resets continuously due to Notification timer that Expired for RF Client: Cat6k QoS Manager.

  Conditions: This symptom is observed on a Cisco 7600 HA loaded with scale QoS and GRE + IPsec configurations.

  Workaround: There is no workaround.

- CSCtx66046

  Symptoms: The Standby RP crashes with a traceback listing db_free_check.

  Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.

  Workaround: Before removing the address, remove the network statement which covers he address of the loopback interface.

- CSCtx67474

  Symptoms: Update message is sent with an empty NLRI when the message consists of 2byte aspath in ASPATH attribute and 4byte value aggregate attribute.

  Conditions: This can happen when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.

  Workaround: Move all the 2byte AS peers to a separate update-group using a non-impacting outbound policy like “advertisement-interval”.

- CSCtx73612

  Symptoms: A Cisco ASR 1000 may reload while reading IPsec MIBs via SNMP and write a crashfile.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.1(1)S1.

  Workaround: Do not poll or trap IPsec information via SNMP.

- CSCtx77501

  Symptoms: Traffic is dropped at decap side of PE box.

  Conditions: This symptom occurs with SSO at decap side of MVPN set-up, DFC core-facing, 6748 access facing.

  Workaround: Do a switchover.

- CSCtx77750

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

  Conditions: CUCM is configured to do Multicast MoH.

  Workaround:

  1. Disable H.323 Multicast MoH functionality in IOS or use SIP Multicast MoH.
  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

- CSCtx79462

  Symptoms: OSPF neighborship does not get established.

  Conditions: This symptom is observed when Enabling PFC on a multilink bundle in SIP-400. The OSPF neighborship does not get established.

  Workaround: There is no workaround. Disable PFC to bring up the OSPF neighborship.

  Further Problem Description: The OSPF hello packets get dropped by the peer end because the IP header is corrupted.

- CSCtx82775

  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.

  Conditions: The symptom is observed when MTP is invoked for calls.

  Workaround: Reload the router or perform a no sccp/sccp.

- CSCtx92802

  Symptoms: IP fragmented traffic destined for crypto tunnel is dropped.

  Conditions: The symptom is observed under the following conditions:

  - Cisco IOS Release 15.0(1)M7 on a Cisco 1841.
  - VRF enabled.
  - CEF enabled.
  - VPN tunnel.

  Workaround: Disable VFR or CEF.

- CSCtx95840

  Symptoms: A Cisco voice gateway may unexpectedly reload.

  Conditions: The symptom is observed on a Cisco voice gateway running SIP protocol. In this case the issue was when sipSPIUfreeOneCCB() returns, the leftover event is still being processed after CCB is released from sipSPIUfreeOneCCB(). Based on sipSPIStartRemoveTransTimer(ccb), CCB should have been released later by a background timer.

  Workaround: There is no workaround.

- CSCty01237

  Symptoms: The router logs show:

  ```
  <timestamp> %OER_BR-5-NOTICE: Prefix Learning STARTED
  CMD: 'show run' <timestamp>
  ```

  This is followed by the router crashing.

  Conditions: This issue is seen under the following conditions:

  1. Configure PfR with a learn-list using a prefix-list as a filter and enable learn.
  2. Use a configuration tool, script or NMS that periodically executes **show run** on the MC over HTTP or some other means.

  Workaround 1: If you use PfR learn-list feature, do not execute **show run** periodically.

  Workaround 2: If you use a monitoring tool that executes **show run** periodically, avoid using a learn-list configuration in PfR.

- CSCty03745

  Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.

  Conditions: This symptom occurs when the IPv4 default route exists, that is:

  ```
  ip route 0.0.0.0 0.0.0.0 <next-hop>.
  ```

  Or a certain static/IGP route exists: For example:

  ```
  ip route 0.0.253.0 255.255.255.0 <next-hop>.
  ```

  Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family. address-family. For example:

  ```
  router bgp 65000
    address-family l2vpn vpls
     neighbor 10.10.10.10 next-hop-self
  ```

  Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

- CSCty05092

  Symptoms: EIGRP advertises the connected route of an interface which is shut down.

  Conditions: This symptom is observed under the following conditions:

  - Configure EIGRP on an interface.
  - Configure an IP address with a supernet mask on the above interface.
  - Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.

  Workaround 1: Remove and add INTERFACE VLAN xx.

  Workaround 2: Clear ip eigrp topology x.x.x.x/y.

- CSCty08070

  Symptoms: Router may print error message and traceback similar to the following example:

  ```
  %SCHED-STBY-3-THRASHING: Process thrashing on watched
  boolean 'OSPFv3 Router
  boolean'. -Process= "OSPFv3R-10/4/2", ipl= 5, pid= 830router ospf
  ```

```
-Traceback= 7235C3Cz 7235F1Cz 6A5F7A8z 6A6168Cz 50DA290z 50D3B44zv
```

Conditions: The symptom is observed when the affected OSPFv3 router is configured, but the process does not run because it has no router-id configured. Further, an area command is configured, for example “area X stub”.

Workaround: Configure “router-id” so the process can run.

- CSCty16620

  Symptoms: Backup pseudowire in SVIEoMPLS does not come up after reloading the router.

  Conditions: This symptom is seen under the following conditions:

  1. Remote PE on the backup PW does not support pseudowire status TLV.
  2. The “no status TLV” is not configured in pw-class used in the PW, which does not support pseudowire status TLV.

  Workarounds:

  Proactive workaround: Configure “no status TLV” into the pw-class used if the remote side does not support status TLV.

  Reactive workaround: Reprovision the backup pseudowire after reload.

- CSCty17288

  Symptoms: MIB walk returns looping OID.

  Conditions: The symptom is observed when a media mon policy is configured.

  Workaround: Walk around CiscoMgmt.9999.

- CSCty23747

  Symptoms: MAC address withdrawal messages are not being sent.

  Conditions: This symptom is seen with flapping REP ports on UPE.

  Workaround: There is no workaround.

- CSCty24606

  Symptoms: Under certain circumstances, the Cisco ASR 1000 series router’s ASR CUBE can exhibit stale call legs on the new active after switchover even though media inactivity is configured properly.

  Conditions: This symptom is observed during High Availability and box to box redundancy, and after a failover condition. Some call legs stay in an active state even though no media is flowing on the new active. The call legs can not be removed manually unless by a manual software restart of the whole chassis. The call legs do not impact normal call processing.

  Workaround: There is no workaround.

- CSCty29230

  Symptoms: CMFIB entries are not being programmed on the SP and DFCs. Mroute shows both Accept and OILS, ip mfib output also shows Accept interface and Forwarding interface, but CMFIB entries are not programmed.

  Conditions: Cisco 7600 running a Cisco IOS Release 15.1(3)S throttle.

  Workaround: There is no workaround.

- CSCty30886

  Symptoms: A standby RP reloads.

Conditions: This symptom is observed when bringing up PPPoE sessions with configured invalid local IP address pool under virtual-template profile and “aaa authorization network default group radius” on the box with no radius present. No IP address is assigned to PPPoE Client.

Workaround: There is no workaround.

- CSCty32463

  Symptoms: When you boot an ASR-1002-X or an ASR-1001 in dual IOSd mode (SSO), the standby process comes up and SSO gets executed but the configuration is unable to sync up between the two processes:

```
%REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
(raw-event=PEER_FOUND(4))
%REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
(raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

%LICENSE-3-BULK_SYNC_FAILED: License bulk sync operation Priority Sync for
feature adventerprise 1.0 failed on standby rc=Remote tty failed
%ISSU-3-INCOMPATIBLE_PEER_UID: Setting image (X86_64_LINUX_IOSD-UNIVERSALK9-
M),
version (15.2(20120222:153818)156) on peer uid (49) as incompatible
Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
  show redundancy config-sync failures mcl

Config Sync: Starting lines from MCL file:
crypto pki certificate chain root-tank.com
 ! <submode> "crypto-ca-cert-chain"

Cannot finish user input data read from fd 17
%RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
kp_perf1>
```

  When this part of the configuration is removed, the issue is not seen:

```
crypto pki certificate chain root-tank.com
! <submode> "crypto-ca-cert-chain"
- ^C
! </submode> "crypto-ca-cert-chain"
```

  Conditions: The position of the ^C is causing the issue.

  Workaround: The starting “^C” should be placed at the same line as “certificate ca”. For example:

```
certificate ca ^C
44AFB080D6A327BA893039862EF8406B
 ......
quit^C
```

- CSCty32728

  Symptoms: CPU hog is seen when MVPN configuration is replaced with another using the **configure replace** command.

Conditions: This symptom is observed on a stable MVPN network when replacing the configuration with dual-home receiver/source configuration once the router comes up with the tunnel.

Workaround: There is no workaround.

- CSCty32851

  Symptoms: A Cisco router may unexpectedly reload due to software forced crash exception when changing the encapsulation on a serial interface to “multilink ppp”.

  Conditions: The symptom is observed when the interface is configured with a VRF.

  Workaround: Shut down the interface before making the encap configuration change.

- CSCty34020

  Symptoms: A Cisco 7201 router’s GigabitEthernet0/3 port may randomly stop forwarding traffic.

  Conditions: This only occurs on Gig0/3 and possibly Fa0/0 as they both are based on different hardware separate from the first three built-in gig ports.

  Workaround: Use ports Gig0/0-Gig 0/2.

- CSCty34200

  Symptoms: In MVPN scale environment, a crash is observed after “no ip multicast-routing”. A memory leak is observed after changing data MDT address.

  Conditions: This symptom is seen in MVPN scale scenario.

  Workaround: There is no workaround.

- CSCty35134

  Symptoms: Data traffic out of REP EdgeNoNeighbor fails to flow.

  Conditions: This symptom is observed when MST runs on the node when “rep stcn stp” is configured. If the MST puts this port to BLK then REP EdgeNN stops forwarding traffic.

  Workaround: When having “rep stcn stp” configured on the rep port, we should not have a topology such that MST puts this port to blocking.

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

  Workaround: There is no workaround.

- CSCty48870

  Symptoms: Router crash due to a bus error.

  Conditions: This has been observed in router that is running Cisco IOS Release 15.2(2)T and 15.2(3)T with NBAR enabled on a crypto-enabled interface. NBAR can be enabled through NAT, QoS, or NBAR protocol discovery.

  Workaround: Using **no ip nat service nbar** will help where NBAR is enabled through NAT.

- CSCty49656

  Symptoms: A crash is observed when executing the **no ip routing** command.

  Conditions: This symptom is observed under the following conditions:

  1. Use a Cisco IOS image that has fix for CSCtg94470.

2. Configure OSPF.
3. Enable multicast.
4. Create several (>6000) routes in the network to be learned by OSPF.
5. Wait for OSPF to learn all the (>6000) routes from the network.

Finally, executing the **no ip routing** command may crash the box.

Workaround: There is no workaround.

- CSCty51088

  Symptoms: On a Cisco ME 3600X or Cisco ME 3800X, when traffic for a group (S2,G) is sent to an interface that is already acting as the source for another group (S1,G), it does not receive any traffic since no (S2,G) entry is formed.

  Conditions: This symptom is observed when the receiver interface is already a source interface for another multicast stream.

  Workaround: There is no workaround.

- CSCty53243

  Symptoms: Video call fails in the latest mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has the uc_infra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.

  Conditions: This symptom is observed when CUBE changes the video port to “0” in 200 OK sent to the UAC.

  Workaround: There is no workaround.

- CSCty54319

  Symptoms: OSPF and protocols using 224.0.0.x will not work btw CE-CE over a VLAN.

  Conditions: This symptom occurs when IGMP snooping is disabled.

  Workaround: Toggle IGMP snooping two times.

- CSCty55449

  Symptoms: The device crashes after registering an Embedded Event Manager TCL policy.

  Conditions: If the policy uses the multiple event feature and the trigger portion is registered without curly braces (“{}”), then the device will crash. For example, this policy will trigger a crash:

```
::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger
::cisco::eem::correlate event 1 or event 2

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

action_syslog priority crit msg " triggered "
```

  Note how “::cisco::eem::trigger” is not followed by an opening curly brace.

  Workaround: Ensure that the trigger portion (i.e.: the correlate statement) is enclosed within curly braces. Given the example above, the proper syntax is:

```
::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger {
    ::cisco::eem::correlate event 1 or event 2
}

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

action_syslog priority crit msg " triggered "
```

- CSCty58241

  Symptoms: The following symptoms are observed:

  Symptom 1. You may receive the following error when you enable radius debugs:

  RADIUS: Response for non-existent request ident

  Symptom 2. The radius alias functionality may not work.

  Conditions:

  For symptom 1: You move from the alias-based configuration to non-alias based configuration and you remove the host first and alias next. In the new configuration if one of the alias becomes the primary host address this will lead to symptom 1.

  For symptom 2: If the reply comes from the alias IP address the functionality may not work.

  Workarounds:

  For symptom 1: - Reload the router; or - Unconfigure the alias first before unconfiguring the host.

  For symptom 2: - Do not use the alias on the NAS.

- CSCty58992

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

  Conditions: This symptom is observed under the following conditions:

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

  Workaround: There is no workaround.

- CSCty63868

  Symptoms: CUBE crashes at sipSPICheckHeaderSupport.

  Conditions: CUBE crashes while running the codenomicon suite.

  Workaround: There is no workaround.

- CSCty64721

  Symptoms: Improper memory allocation by CTI process crashes the CME.

  Conditions: The CTI front end process is using up huge memory causing the CME to crash eventually. When the crash occurs:

```
Processor Pool Total:  140331892 Used:  140150164 Free:     181728
      I/O Pool Total:   27262976 Used:    5508816 Free:   21754160
```

  Workaround: There is no workaround.

- CSCty68348

  Symptoms: If the OSPF v2 process is configured with the **nsr** command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

  Conditions: This symptom is observed under the following conditions:

  – The OSPF router is configured for “nsr”.

  – Shutdown/no shutdown of the OSPF process.

  Workaround: Flapping of the neighbor will fix the issue.

- CSCty68402

  Symptoms: NTT model 4 configurations are not taking effect.

  Conditions: This symptom occurs under the following conditions:

```
policy-map sub-interface-account
 class prec1
  police cir 4000000 conform-action transmit  exceed-action drop
  account
 class prec2
  police cir 3500000 conform-action transmit  exceed-action drop
  account
 class prec3
  account
 class class-default fragment prec4
  bandwidth remaining ratio 1
  account

policy-map main-interface
 class prec1
  priority level 1
  queue-limit 86 packets
 class prec2
  priority level 2
  queue-limit 78 packets
 class prec3
 bandwidth remaining ratio 1
  random-detect
  queue-limit 70 packets
  class prec4 service-fragment prec4
  shape average 200000
  bandwidth remaining ratio 1
  queue-limit 62 packets
 class class-default
  queue-limit 80 packets
```

  Workaround: There is no workaround.

- CSCty71843

  Symptoms: Tracebacks observed at lfd_sm_start and lfd_sm_handle_event_state_stopped APIs during router bootup.

  Conditions: The symptom is observed with L2VPN (Xconnect with MPLS encapsulation) functionality on a Cisco 1941 router (acting as edge) running Cisco IOS interim Release 15.2(3.3)T. This is observed when a router is reloaded with the L2VPN configurations.

  Workaround: There is no workaround.

- CSCty73817

  Symptoms: In large-scale PPPoE sessions with QoS, the Standby RP might reboot continuously (until the workaround is applied) after switchover. This issue is seen when the QoS Policy Accounting feature is used. When the issue occurs, the Active RP remains operational and the Standby RP reboots with the following message:

  ```
  %PLATFORM-6-EVENT_LOG: 43 3145575308: *Mar 16 13:47:23.482: %QOS-6-RELOAD: Index
  addition failed, reloading self
  ```

  Conditions: This symptom occurs when all the following conditions are met:

  1. There is a large amount of sessions.
  2. The QoS Policy Accounting feature is used.
  3. Switchover is done.

  Workaround: Bring down sessions before switchover. For example, shut down the physical interfaces that the sessions go through, or issue the Cisco IOS command **clear pppoe all**.

- CSCty76106

  Symptoms: Crash is seen after two days of soaking with traffic.

  Conditions: This symptom occurs with node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, constant frequent polling of SNMP, RCMD, full scale of routes and bidirectional traffic.

  Workaround: There is no workaround.

- CSCty78435

  Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

  Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

  Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- CSCty80553

  Symptoms: Multicast router crashes.

  Conditions: The symptom is observed when multicast traffic is routed through an IPsec tunnel and multicast packets are big causing fragmentation.

  Workaround: Make sure that multicast packet sizes do not exceed tunnel transport MTU.

- CSCty81700

  Symptoms: When a remote PE reloads in MVPN network, it causes a memory leak.

Conditions: This symptom occurs when core interface flap or remote PE node reloads causing a small amount of memory leak. If the node stays up experiencing a lot of core interface/remote PE outages, it can run out of memory and fail to establish PIM neighborship with remote PEs.

Workaround: There is no workaround. As a proactive measure, user can periodically (depending on n/w outages) run the **show memory debug leak chunk** command and reload the node, if there are a lot of memory leaks reported by this command.

- CSCty83357

  Symptoms: ACL denied packets are getting punted to host queue, leading to flaps in routing protocols.

  Conditions: This symptom occurs when ACL is configured with src IP match, and packets are being denied by the ACL. The packets are punted to the CPU.

  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.

- CSCty84989

  Symptoms: IKEv2 pushed routes are not installed in the IPv6 inner VRF routing table.

  Conditions: This symptom occurs when using IKEv2 on pure IPV6 tunnels with tunnel protection IPsec and a VRF on the tunnel.

  Workaround: There is no workaround.

- CSCty85926

  Symptoms: VC (VPLS/EoMPLS) will stay down with the following in the **show mpls l2 vc detail** command:

  Signaling protocol: LDP, peer unknown

  Conditions: This symptom will only happen if you have LDP GR configured. Do a SSO switchover and try configuring the VC after the switchover is complete.

  Workaround: There is no workaround. Reload the switch.

- CSCty86111

  Symptoms: The Cisco ISR G2 router crashes after “no ccm-manager fallback-mgcp” is configured.

  Conditions: This symptom is observed with Cisco ISR G2 router.

  Workaround: There is no workaround.

- CSCty90223

  Symptoms: A crash occurs at nhrp_nhs_recovery_co_destroy during setup and configuration.

Conditions: This symptom is observed under the following conditions:

1. Add and remove the ip nhrp configuration over the tunnel interface on the spoke multiple times.
2. Do shut/no shut on the tunnel interface.
3. Rapidly change IPv6 addresses over the tunnel interface on the spoke side and on the hub side multiple times.
4. Replace the original (correct) IPv6 addresses on both the spoke and the hub.
5. Wait for the registration timer to start.

The crash, while not consistently observed, is seen fairly often with the same steps.

Workaround: There is no known workaround.

- CSCty90293

  Processing improvements for GREv6 over IPv6 currently requires IP CEFv6 to be disabled,

  Workaround: Use “tunnel protection” instead,

- CSCty91955

  Symptoms: L2-switched traffic loss within a BridgeDomain routed traffic via an SVI experiences no loss.

  Conditions: This symptom occurs with BridgeDomain that has both tagged and untagged EVCs. Issue should not happen with like-to-like scenario.

  Workaround: Make sure there is like-to-like (tagged-to-tagged or untagged-to- untagged) communication.

- CSCty94289

  Symptoms: The drop rate is nearly 1 Mbps with priority configuration.

  Conditions: This symptom is observed when traffic received in the MSFC router class-default is the same as on the other end of the MSFC2 router.

  Workaround: Unconfigure the priority and configure the bandwidth, and then check for the offered rate in both the routers. This issue is only seen with the Cisco 7600 series routers (since the issue is with the Flexwan line cards). The issue is seen with a priority configuration and does not show up when the priority is unconfigured, so there is no workaround as such for this issue otherwise.

- CSCty96049

  Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.

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

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

- CSCty96052

  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

  Conditions: It is an extreme corner case/timing issue. Has been observed only once on release image.

  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty96579

  Symptoms: Under periods of transient interface congestion, an MPLS-TP network may experience unnecessary traffic switchovers or longer than expected restoration times.

  Conditions: This symptom is observed during periods of transient interface congestion. Behavior will be caused by loss of vital OAM packets (e.g. AIS/LDI, LKR). Lack of a classification mechanism for these packets prevents from protecting them with a QoS policy.

  Workaround: There is no workaround.

- CSCty97784

  Symptoms: The router crashes.

  Conditions: This symptom is observed when NBAR is enabled, that is, “match protocol” actions in the QoS configuration, or “ip nbar protocol-discovery” on an interface or NAT is enabled and “ip nat service nbar” has not been disabled.

  Workaround: There is no workaround.

- CSCty99331

  Symptoms: CPU hog messages are seen on the console.

  Conditions: This symptom is seen when applying huge rmap with more than 6k sequences on an interface.

  Workaround: There is no workaround.

- CSCty99711

  Symptoms: SIP-400 crash may be observed due to illegal memory access.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SRE4 when SIP-400 has PPPoE session scale.

  Workaround: There is no workaround.

- CSCty99874

  Symptom: Ingress policing is done on the EVC which does not have QoS policy.

  Conditions: This symptom is observed when one EVC has a QoS policy, and another does not. The QoS policy shows effect on the other EVC also.

  Workaround: Attach a dummy policy to the other EVC. Or attach and detach a policy on the other EVC.

- CSCtz01361

  Symptoms: Traffic gets black holed when TE auto-backup is enabled on midpoint router and FFR is configured on the P2MP TE tunnel head end.

  Conditions: This symptom is seen when enabling FRR on the head end with auto- backup already configured on the box.

  Workaround: Remove auto-backup configuration from the midpoint router.

- CSCtz02182

  Symptoms: Tracebacks are seen on a flexVPN hub.

  Conditions: The symptom is observed when adding a virtual-template interface type tunnel.

  Workaround: There is no workaround.

- CSCtz02622

  Symptoms: FlexVPN spoke crashed while passing spoke to spoke traffic.

Conditions: Passing traffic from spoke to spoke or clearing IKE SA on the spoke.

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 6.1/5:

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

CVE ID CVE-2012-3893 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

- CSCtz04090

  Symptoms: In a VRRP/HSRP setup, traffic from particular hosts is getting dropped. Ping from the host to any device through the VRRP routers fails.

  Conditions: This symptom is usually seen after a VRRP/HSRP switchover. The packet drops because of some packet loop that is created between the routers running VRRP/HSRP.

  Workaround: A clear of the MAC table on the new VRRP master usually restores the setup to working conditions.

- CSCtz06611

  Symptoms: IPSec tunnel states are UP-IDLE because of broadcast packets that are punted to the CPU. The mac-address of VPN-SPA is not learned properly.

  Conditions: This symptom is a timing issue. You may see it first time or need to try multiple times. This symptom is seen with crypto map plus vrf configuration.

  1. Reload the router with above configuration: the mac-address changes to all FF.
  2. Default the configuration of VLAN (where crypto map and engine is applied), then configure it again with old configuration. Now the mac-address will show all FF.
  3. Create the vlan. Do a **no shutdown**. Attach vrf. Then add crypto map to it.

  Workarounds: For the steps mentioned in condition section above, below are the workarounds respectively.

  Workaround 1: Remove and add "ip vrf forwarding" and then remove and add the **crypto engine** command.

  Workaround 2: Remove and add the **crypto engine** command.

  Workaround 3: Do a **shut/no shut** on the VLAN interface.

- CSCtz08037

  Symptoms: The router fails to pass any traffic after receiving the "%OCE-3-OCE_FWD_STATE_HANDLE: Limit of oce forward state handle allocation reached; maximum allowable number is 50000" error message.

  Conditions: This symptom is observed MPLS L2VPN is configured with EoMPLSoGRE with IPSec encryption on top of the VTI tunnel with IPSec encryption (double encryption).

  Workaround: Reload the router.

- CSCtz08719

  Symptoms: With split horizon, traffic does not flow on all BDs.

  Conditions: This symptom is observed when traffic does not flow on all BDs.

  Workaround: There is no workaround.

- CSCtz08746

  Symptoms: On the 12in1 Serial SPA with hardware version lower than 2.0, an upgrade using "test upgrade" with the latest Cisco 7600 FPD bundles results in the SPA FPD device being downgraded from version 1.2 to 1.1. Subsequently, both auto and manual upgrades fail to bring the SPA FPD version back to 1.2. The SPA goes to the OutOfServ or FpdUpReqd state.

  Conditions: This issue is seen only with the older SPA hardware (hardware version lower than 2.0) when it is plugged into a SIP200 or SIP400 on the Cisco 7600 platform.

  Workaround: Use the latest SPA hardware (hardware version 2.0 or above).

- CSCtz12714

  Symptoms: A Cisco router configured for voice functions may crash.

  Conditions: The exact conditions to trigger the crash are unknown at this time.

  Workaround: There is no workaround.

- CSCtz13451

  Symptoms: A Cisco ME 3800X and Cisco ME 3600X switch may experience CPU HOG errors and then a watchdog crash or memory corruption.

  Conditions: This symptom is observed when running many of the **show platform mpls handle** commands. The switch may crash.

```
SW#sh platform mpls handle 262836664 ?
  BD_HANDLE              bd/el3idc_vlan handle
 L2VPN_L2_HANDLE        l2 tunnel intf handle
  L2VPN_PW_BIND_DATA     pw bind data
  LFIB_TABLE             LFIB TABLE handle
  PORT_HANDLE            port/met handle
  RW_HANDLE              Rewrite handle
  SW_OBJ_ADJACENCY       oce type SW_OBJ_ADJACENCY
  SW_OBJ_ATOM_DISP       oce type SW_OBJ_ATOM_DISP
  SW_OBJ_ATOM_IMP        oce type SW_OBJ_ATOM_IMP
  SW_OBJ_DEAGGREGATE     oce type SW_OBJ_DEAGGREGATE
  SW_OBJ_EGRESS_LABEL    oce type SW_OBJ_LABEL
 SW_OBJ_EOS_CHOICE      oce type SW_OBJ_EOS_CHOICE
  SW_OBJ_FIB_ENTRY       oce type SW_OBJ_FIB_ENTRY
  SW_OBJ_FRR             oce type SW_OBJ_FRR
  SW_OBJ_GLOBAL_INFO     oce type SW_OBJ_GLOBAL_INFO
  SW_OBJ_ILLEGAL         oce type SW_OBJ_ILLEGAL
  SW_OBJ_IPV4_FIB_TABLE  oce type SW_OBJ_IPV4_FIB_TABLE
  SW_OBJ_IPV6_FIB_TABLE  oce type SW_OBJ_IPV6_FIB_TABLE
  SW_OBJ_LABEL_ENTRY     oce type SW_OBJ_LABEL_ENTRY
  SW_OBJ_LABEL_TABLE     oce type SW_OBJ_LABEL_TABLE
  SW_OBJ_LOADBALANCE     oce type SW_OBJ_LOADBALANCE
  SW_OBJ_RECEIVE         oce type SW_OBJ_RECEIVE
```

  Workaround: Do not run the commands as they are for development use.

- CSCtz13818

  Symptoms: In a rare situation when route-map (export-map) is updated, IOS is not sending refreshed updates to the peer.

  Conditions: The symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.

  Workaround 1: Refresh the updated route-target to use **clear ip route vrf** *vrf-name net mask*.

  Workaround 2: Hard clear the BGP session with the peer.

- CSCtz14634

  Symptoms: Negative “maximum reservable bandwidth” and “priority” values are seen on the opaque-lsa for Bundle-Ether[2*10GE]interface.

  Conditions: This symptom is observed on the Bundle-Ether[2*10GE]interface.

  Workaround: There is no workaround. The error is only in the way the values are displayed by **show** commands. The correct bandwidth values are sent in the opaque LSA, and this error has no operational effect.

- CSCtz14980

  Symptoms: When you perform the RP switch, the standby RP (original active one) will keep rebooting.

  Conditions: The symptom is observed when you have “crypto map GETVPN_MAP gdoi fail-close” configured and image is Cisco IOS XE Release 3.6 or 3.7.

  Workaround: There is no workaround.

- CSCtz15211

  Symptoms: The ISM card does not encrypt packets through a double encrypted tunnel.

  Conditions: This symptom is observed with ISR g2 with the ISM module and crypto configured for GRE over IPsec packets to be encrypted through a VTI (double encryption).

  Workaround: Use onboard encryption.

- CSCtz16622

  Symptoms: A Cisco ME 3600X acts as a label disposition Edge-LSR when receiving MPLS packets with Checksum 0xFFFF that will continue to drop with Ipv4HeaderErr and Ipv4ChecksumError at nile.

  Conditions: This symptom is seen with label pop action at the Edge-LSR.

  Workaround: There is no workaround.

- CSCtz22112

  Symptoms: A VXML gateway may crash while parsing through an HTTP packet that contains the “HttpOnly” field:

  ```
  //324809//HTTPC:/httpc_cookie_parse: * cookie_tag=’ HttpOnly’
  //324809//HTTPC:/httpc_cookie_parse: ignore unknown attribute: HttpOnly
  Unexpected exception to CPU: vector D, PC = 0x41357F8
  ```

  Note: The above log was captured with “debug http client all” enabled to generate additional debugging output relevant to HTTP packet handling.

  Conditions: The symptom is observed when an HTTP packet with the “HttpOnly” field set is received.

Workaround: There is no workaround.

- CSCtz23433

  Symptoms: ISG shell maps with policer on egress child default-class fail.

  Conditions: This symptom is seen with shell map with policer or shaper on child default-class.

  Workaround: There is no workaround.

- CSCtz24047

  Symptoms: Free process memory is being depleted slowly on line cards in the presence of the DLFIoATM feature configured on a PA-A6-OC3 (enhanced Flexwan). Finally memory allocation failures are observed. Use the **show memory proc stat history** command to display the history of free process memory.

  Conditions: Slow Proc Memory depletion is observed on 7600-ES+ cards when installed on a Cisco 7600 router that has DLFIoATM configured on a PA-A6-OC3 hosted on an enhanced Flexwan module.

  Workaround: There is no workaround.

- CSCtz25953

  Symptoms: “LFD CORRUPT PKT” error message is dumped and certain length packets are getting dropped.

  Conditions: The symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

  Workaround: There is no workaround.

- CSCtz26188

  Symptoms: Packet loss is observed on platforms in certain deployments having a large number of prefixes routing traffic onto a TE tunnel.

  Conditions: If the Configured value of the cleanup timer is 60 secs, then packets might be lost on the platforms where the forwarding updates take longer.

  Workaround: Configure the value of the cleanup timer to 300secs.

  mpls traffic-eng reoptimize timers delay cleanup 300

- CSCtz27782

  Symptoms: A crash is observed on defaulting service instance with OFM on EVC BD configured.

  Conditions: This symptom occurs when interface is in OAM RLB slave mode.

  Workaround: There is no workaround.

- CSCtz30983

  Symptoms: Crash on ES+ line card upon issuing the “show hw-module slot X tech- support” or “show platform hardware version” command.

  Conditions: This symptom occurs on an ES+ line card.

  Workaround: Do not issue the **show hw-module slot X tech-support** or **show platform hardware version** command on an ES line card unless explicitly mentioned by Cisco.

- CSCtz31888

  Symptoms: After state change of one of the L3 uplink interfaces, STP cost of BPDU PW increases from 200 to 2M, which can lead to blocking state in STP for this PW.

  Conditions: This symptom occurs with state change of one of the uplink L3 interfaces.

Workaround: Increase the cost of access ring to more then 2M to avoid blocking of the BPDU PW.

- CSCtz32521

  Symptoms: In interop scenarios between Cisco CPT and Cisco ASR 9000 platforms, in order to support transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Conditions: This symptom occurs in interop scenarios between Cisco CPT and Cisco ASR 9000 platform. In order to support transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Workaround: There is no workaround.

- CSCtz33536

  Symptoms: SIP KPML subscription fails with:

  ```
  ?xml version="1.0" encoding="UTF-8"?><kpml-response version="1.0" code="533"
  text="Multiple Subscriptions on a Dialog Not Supported"/
  ```

  This happens on a CUBE when the call is transferred on CUCM.

  Conditions: The symptom is observed with SIP to SIP CUBE running Cisco IOS Release 15.1(3)T2.

  Workaround: Use a different DTMF method.

- CSCtz35061

  Symptoms: Flexlink switchover causes VLAN to not be allowed in trunk link.

  Conditions: This issue is related to flexlink switchover caused by instantaneous link flapping.

  Workaround: There is no workaround.

- CSCtz35467

  Symptoms: QoS policy-map gets detached from interface on line protocol down-- >up transition happens on reload, admin shut/no shut and interface flap as well.

  Conditions: This symptom is observed when QoS policy-map is applied at interface and more than one child has “priority + police cir percent x” configured.

  Workaround: To be preventive use “police cir <absolute>” instead of “police cir percent x”. To be reactive use EEM applet/script.

  Further Problem Description: There is no error message in the syslog, only on console. It seems that line protocol UP can be used as the trigger action for EEM.

- CSCtz37863

  Symptoms: IPCP is not in an open state and it does not seem to be calling the This-Layer-Down (TLD) vector.

  Conditions: The symptom is observed if IPv4 saving is enabled and IPCP negotiation failed because of a TermReq received from peer.

  Workaround: There is no workaround.

- CSCtz38119

  Symptom: The router does not complete a MAC address flush on the receiving side of a VPLS pseudowire.

  Conditions: Occurs when the router receives a layer 2 MAC withdrawal over a VPLS pseudowire.

  Workaround: There is no workaround.

- CSCtz40435

  Symptoms: The L4 port-range security ACL does not work on EVC.

  Conditions: This symptom is seen when security ACL containing L4 port range operation that is applied on EVC. The behavior is not as expected. The same works on physical interface.

  Workaround: Add support for L4 port range operation similar to the case of applying it on physical interface.

  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

- CSCtz40621

  Symptoms: Router crash observed.

  Conditions: The symptom is observed when GetVPN GM tries to register to keyserver and keyserver issues a rekey simultaneously.

  Workaround: There is no workaround.

- CSCtz41048

  Symptoms: The **trace mpls ipv4** command is unsuccessful.

  Conditions: The symptom is observed with the **trace mpls ipv4** command.

  Workaround: There is no workaround.

- CSCtz45057

  Symptoms: High CPU is seen on a Cisco ME 3800X switch.

  Conditions: This symptom occurs when loop of OTNIFMIB causes CPU Hog/Crash on a Cisco ME 3800X switch during pulling from PPM.

  Workaround: Disable OTNIFMIB while pulling from PPM, which is not supported or required on Cisco ME 3800X and ME 3600X switches.

- CSCtz45487

  Symptoms: REP flaps when modifying allows VLANs on REP enabled trunk.

  Conditions: This symptom is seen under the following conditions:

  - "vlan dot1q tag native" must be configured globally.
  - Issue does not occur when native VLAN is 1 on REP trunk.
  - Issue is seen on Cisco IOS Releases 15.2(2)S, 15.1(2)EY2a and earlier Cisco IOS 15.1(2)S releases.
  - Issue is not seen on Cisco IOS Release 12.2(52)EY4 and earlier Cisco IOS 12.2(52)EY releases.

  Workaround:

  - Remove "vlan dot1q tag native" global configuration.
  - Change to native VLAN 1 on the REP enabled trunks.
  - Change to Cisco IOS Release 12.2(52)EY.

- CSCtz45901

  Symptoms: The **show runn** or **format xml** output for an ATM interface is not displayed in the correct order.

  Conditions: The symptom is observed if there are multiple subinterfaces for an ATM interface and PVC is configured under these.

  Workaround: There is no workaround.

- CSCtz46300

  Symptoms: Traffic is not classified under the QoS ACLs having port matching using range (inclusive range), lt (less than), and gt (greater than) operators.

  Conditions: This symptom is seen with IPv4 and IPv6 with L4 port ranger operations using range, lt, and gt, which do not work with QoS ACLs on Cisco ME 3600 and Cisco ME3800 switches.

  Workaround: There is no workaround.

- CSCtz47873

  Symptoms: The command **show crypto ikev2 client flex** does not work as expected.

  Conditions: The symptom is observed with a client/server flexVPN setup.

  Workaround: Execute either **show crypto IKEv2 sa** or **show crypto session detail**.

- CSCtz48615

  Symptoms: AES encryption may cause high CPU utilization at crypto engine process.

  Conditions: The symptom is observed with AES encryption configuration in ISAKMP policy. The issue is seen only when one of the negotiating routers is a non-Cisco device where the key size attribute is not sent in ISAKMP proposal.

  Workaround: Remove ISAKMP policy with AES encryption.

- CSCtz54823

  Symptoms: Configuration is getting locked on chopper SPA.

  Conditions: This symptom happens as follows:

  1. Shut down the controller of the SPA.
  2. Reload will bring the SPA in the locked state.

  Workaround: There is no workaround. Erase start up and reload the system to get back to configuration mode.

- CSCtz59429

  Symptoms: Packets do not match a flow with the attribute “application category voice-video”.

  Conditions: This symptom occurs when a flow with the attribute “application category voice-video” is matched for the same attribute.

  Workaround: There is no workaround.

- CSCtz62680

  Symptoms: “DFC WAN Line Card Software Element Not Found - QOS: TCAM Class ID” errors appear along with BADCHUNKFREEMAGIC errors, leading to an ES20 crash.

  Conditions: When service policies less than 128 kb are added or removed.

  Workaround: There is no workaround.

- CSCtz66770

  Symptoms: When under ATM PVC (SPA-4XOC3-ATM or v2) with MUX encapsulation and OAM enabled, L3 policy-map is applied and PVC goes down.

  Conditions: This symptom occurs when policy-map sets DSCP (to 7) for default- class, and it affects OAM communication.

  Workaround: Use aal5snap encapsulation.

- CSCtz67403

  Symptoms: A Cisco ME 3600 switch as core switch is dropping all BPDU coming in QnQ tunnel.

  Conditions: This symptom occurs on a Cisco ME 3600 switch that is the core, and the Cisco ME 3400 switches are edge switches.

  Workaround: There is no workaround.

- CSCtz67726

  Symptoms:

  1. Single probe ID is not permitted on the **ip sla group schedule...** command. For example: **ip sla group schedule** *group id* **schedule-period 5 start now** gives following error messages:

     ```
     %Group Scheduler: probe list wrong syntax

     %Group schedule string of probe ID's incorrect
     ```

  2. Entering the same probe ID under **ip sla group schedule** in the format of "id,id" is accepted but it will display on the running configuration as just single probe ID. For example: **ip sla group schedule** *group* **id,id schedule-period 5 start now**. The running configuration will show **ip sla group schedule** *group* **id schedule-period 5 start now**.

  Conditions: Observed if using single probe ID under **ip sla group schedule...** command.

  Workaround: Use the command **ip sla schedule** for single probe ID.

- CSCtz72044

  Symptoms: EzVPN client router is failing to renew ISAKMP security association, causing the tunnel to go down.

  Conditions: The issue is timing-dependent, therefore the problem is not systematic.

  Workaround: There is no workaround.

- CSCtz72390

  Symptoms: The name mangling functionality is broken. Authorization fails with the "IKEv2:AAA group author request failed" debug message.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T.

  Workaround: There is no workaround.

- CSCtz72615

  Symptoms: All interfaces on a Cisco 7600-SIP-200 are down after Cisco IOS downgrade.

  Conditions: This symptom is observed on Cisco 7600 series routers.

  Workaround: There is no workaround.

- CSCtz73157

  Symptoms: CUBE sends 0.0.0.0 when 9971 has video enabled for hold/resume/conference from PSTN caller. CUBE sends correct IP address when 9971 has video disabled for hold/resume/conference from PSTN caller.

Conditions: The symptom is observed with the following conditions:

- Cisco IOS Release 15.2(2)T1.
- Current phone load sip99719.2.4-19.
- Current CUCM version: 8.5.1.13900-5.
- MCS7825I4-K9-CMD2A.
- On the SIP trunk, the box “Retry Video Call as Audio” was checked.

For the calls with video disabled, the CUBE is sending the 200OK with the C=IN ipX x.x.x.x address.

```
Sent:
SIP/2.0 200 OK
Via: SIP/2.0/TCP x.x.x.x:5060;branch=z9hG4bK7322e28fb58f2
From: "name"
<sip:2127153896@x.x.x.x>;tag=1171271~17954349-bc2a-4081-adb4-34491012bb45-24984725
To: <sip:16464831236@x.x.x.x>;tag=D99A474-A1A
Date: Tue, 24 Apr 2012 18:26:17 GMT
Call-ID: f9e43000-f961f049-61593-a28050a@x.x.x.x
CSeq: 101 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:16464831236@x.x.x.x>;party=called;screen=no;privacy=off
Contact: <sip:16464831236@x.x.x.x:5060;transport=tcp>
Supported: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.2.T1
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 241

v=0
o=CiscoSystemsSIP-GW-UserAgent 9798 5431 IN IPX x.x.x.x
s=SIP Call
c=IN IPX x.x.x.x
t=0 0
m=audio 25014 RTP/AVP 0 101
c=IN IPX x.x.x.x
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

For the calls with video enabled, the CUBE is not sending the IP address correctly, as seen here:

```
Sent:
SIP/2.0 200 OK
```

```
Via: SIP/2.0/TCP x.x.x.x:5060;branch=z9hG4bK734ab4c88ccb9
From: "name"
<sip:2127153896@x.x.x.x>;tag=1171897~17954349-bc2a-4081-adb4-34491012bb45-24984949
To: <sip:164648312236@x.x.x.x>;tag=DA1D53C-2232
Date: Tue, 24 Apr 2012 18:35:25 GMT
Call-ID: 39f7e280-f961f262-616f4-a28050a@x.x.x.x
CSeq: 102 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, INFO, REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:164648312236@x.x.x.x>;party=called;screen=no;privacy=off
Contact: <sip:164648312236@x.x.x.x:5060;transport=tcp>
Supported: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.2.2.T1
Supported: timer
Content-Type: application/sdp
Content-Length: 278

v=0
o=CiscoSystemsSIP-GW-UserAgent 144 2583 IN IPX x.x.x.x
s=SIP Call
c=IN IPX 0.0.0.0
t=0 0
m=audio 16654 RTP/AVP 0 101
c=IN IPX 0.0.0.0
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
m=video 0 RTP/AVP 126
c=IN IPX 10.5.40.14
```

Workaround: Disable video from CUCM phone page under the 9971.

- CSCtz74189

  Symptoms: Occasionally the system hangs at bootup with the following signature in the bootlogs. The system will not respond to break character keys.

```
Configuring Freq Synthesizer 2^M
Synthesizer PLL 2 locked successfully^M
Configuring Freq Synthesizer 3^M
Synthesizer PLL 3 locked successfully^M
Configuring Freq Synthesizer 4^M
Synthesizer PLL 4 locked successfully^M
TDM Processor has been configured in iter(1)^M <<<<<<<<<<< HANG
```

  Conditions: This symptom occurs in normal reload conditions, or on a next reload of the software after a system power cycle.

Workaround: Requires a system power cycle.

- CSCtz74685

  Symptoms: A router crash is observed on Y1731 DM.

  Conditions: This symptom is seen when starting 1DM session.

  Workaround: There is no workaround.

- CSCtz75228

  Symptoms: On a power cycle or a reload condition, the system may stall occasionally after the following console logs are printed.

```
<snip
Finished memctrl.h, apply WinHMS Errata...
Initialize Winpath
Initializing interrupt controller
Initialization of Winpath Complete
loading program at addr: 0xE2C00000, size: 0x0007A648
Enable the MIPS Core0
Before minimon_init() call... <<<<<<<<<<HANG
-----  minimon 1st 64 bytes ------
C00BD108:
```

  Conditions: This symptom may happen during a system reload.

  Workaround: A power cycle is required, and the subsequent reload may not be impacted.

- CSCtz75380

  Symptoms: A Cisco ASR 1000 series router sends malformed radius packets during retransmission or failover to a secondary radius server, e.g.: Cisco CAR.

  ISG log if secondary radius server is installed in the network:

```
Radius-Server Log:
13:23:01.011: P78: Packet received from 10.0.0.1
13:23:01.011: P78: Packet successfully added
13:23:01.011: P78: Parse Failed: Invalid length field - 63739 is greater than 288
13:23:01.011: Log: Packet from 10.0.0.1: parse failed <unknown user>
13:23:01.011: P78: Rejecting Request: packet failed to parse
13:23:01.011: P78: Trace of Access-Reject packet
13:23:01.011: P78:    identifier = 40
13:23:01.011: P78:    length = 21
13:23:01.011: P78:    reqauth = 23:<snip....>
13:23:01.011: P78: Sending response to 10.0.0.1
13:23:01.011: Log: Request from 10.0.0.1: User <unknown user> rejected
(MalformedRequest).
13:23:01.011: P78: Packet successfully removed
```

  Conditions: The issue can occur during retransmission of radius access requests or if radius packets are sent to a secondary radius server.

  Workaround: There is no workaround.

- CSCtz76650

  Symptoms: In phase 2 IPv6 DMVPN deployment, traffic for IPv6 hosts behind spokes goes via the hub.

  Conditions: This symptom is observed in IPv6 DMVPN network when using phase 2 configuration and routing protocols with link-local nexthop.

  Workaround: Do not use link-local nexthop routing, instead use unicast nexthops (e.g.: BGP as the routing protocol).

- CSCtz77171

  Symptoms: Subscriber drops are not reported in mod4 accounting.

  Conditions: This symptom is observed on checking policy-map interface for account QoS statistics on a port-channel subinterface.

  Workaround: There is no workaround.

- CSCtz78194

  Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.

  Conditions: The symptom is observed with the Cisco ASR configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.

  Workaround: Shorten the ISAKMP profile name to less than 31.

- CSCtz80643

  Symptoms: A PPPoE client's host address is installed in the LNS's VRF routing table with the **ip vrf receive** *vrf name* command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

  Conditions: This symptom is observed only when the Virtual-access interface is configured with the **ip vrf receive** *vrf name* command via the Virtual-Template or RADIUS profile.

  Workaround: There is no workaround.

- CSCtz83311

  Symptoms: In the bootlog, the following strings may be observed:

  ```
  "MCB timeout"
  ```

  Occasionally these messages also are followed by a GigE port link down for any of the ports Gig 0/1-Gig 0/8. A **shut/no shut** may not recover the link down condition.

  Conditions: This symptom happens during a system reload. It may also happen if a **media-type** command is issued to the first eight GigE ports.

  Workaround: Do not configure "media-type rj45" for the first eight ports either at bootup time or configurations if you are using an image that does not have this fix.

- CSCtz85907

  Symptoms: A Cisco 7600 should have an MVPNv4 configuration and the system replication mode as egress. Now if "address-family ipv6" is configured under the VRF definition, MVPN traffic might be affected.

  Conditions: SREx and RLSx releases.

  Workaround: Use ingress replication.

- CSCtz86024

  Symptoms: There is a long delay in joining mcast stream with Cisco IOS 15S releases that are running on RP.

  Conditions: This symptom is seen when there is no (*,G) on the box, and the first packet for the stream creates this entry.

  Workaround: With static joins we can make sure that entry is present in mroute table.

- CSCtz86747

  Symptoms: Router crashes upon removing all the class-maps from policy-map.

  Conditions: This symptom is observed when a route crashes while removing all user defined class-maps with live traffic.

  Workaround: Shut the interface first before removing class-map.

- CSCtz86763

  Symptoms: Sessions remain partially created, and memory is consumed and not returned.

  Conditions: This symptom occurs when sessions are churned and reset before they reach active state.

  Workaround: There is no workaround.

- CSCtz88289

  Symptoms: It is observed that in a Cisco ME 3600-24CX unit, which is subjected to 100 consecutive image reloads, there is a system bootup hang in this area. The system stalls indefinitely and does not respond to console keystrokes like break keys.

  ```
  <bootup snip>


   I2C Bus Initialization begins
   Margining CPU and Nile board Voltages
   Control FPGA Initialization begins  <<<<System  Hang here
  ```

  Conditions: This symptom may happen during a system bootup.

  Workaround: A powercycle is required, and the next reload may not hit the above condition.

- CSCtz89608

  Symptoms: A router that is operating in an ISG environment experiences a crash due to memory corruption.

  Conditions: This symptom occurs within the SSS context.

  Workaround: There is no workaround.

- CSCtz90154

  Symptoms: Rapid getVPN re-registration by GM when IPsec failure occurs during initial registration. Multiple ISAKMP SAs created and deleted per second.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.2(1)S or Release 15.2(1)S2 as a GM.

  Workaround: There is no workaround.

- CSCtz90909

  Symptoms: A router crashes while giving the **no l2 vfi** *vfi-name* **point-to-point** command.

  Conditions: This symptom occurs while unconfiguring l2 vfi. The router crashes.

  Workaround: There is no workaround.

- CSCtz94188

  Symptoms: With AdvancedMetroIPAccess evaluation license and with TDM permanent license xconnect under CEM, ckts are not shown and are not configurable.

  Conditions: This symptom occurs under regular configuration steps.

  Workaround: There is no workaround.

- CSCtz96342

  Symptoms: Inconsistency in scaled feature license name between Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* and Cisco IOS Release 15.2(2)S:

  Cisco IOS Releases 12.2(52)EY*/15.1(2)EY* - ScaledServices

  Cisco IOS Release 15.2(2)S - ScaledMetroAggrServices

  Conditions: This symptom occurs with an upgrade from Cisco IOS Releases 12.2 (52)EY*/15.1(2)EY* to Cisco IOS Release 15.2(2)S release, which could impact the scalability feature in below ways:

  – If user already had permanent license before upgrade, it will now downgrade to Eval license.
  – New license for installing ScaledMetroAggrServices cannot be generated as the license tool does not support this feature name.

  Workaround: Upgrade to Cisco IOS Release 15.2(2)S1.

- CSCtz97244

  Symptoms: IPSLA Video Operation with VRF support sees no packets received at responder.

  Conditions: This symptom occurs when no emulate CLI is specified with the input interface.

  Workaround: Use the emulate CLI to specify the input interface that has access to the VRF.

- CSCtz97755

  Symptoms: ES card crash and alignment tracebacks on SP are seen.

  Conditions: This symptom is observed with IPv6 unicast and multicast traffic up and running. Unconfiguring IPv6 unicast-routing will lead to this issue.

  Workaround: There is no workaround.

- CSCua01375

  Symptoms: Certificate validation fails when CRL is not retrieved.

  Conditions: This symptom occurs when the router is configured to use a VRF.

  Workaround: Use certificate map to revoke certificates or publish CRL to an HTTP server and configure “CDP override” to fetch the CRL.

- CSCua10377

  Symptoms: A Cisco router with Circuit Emulation SPA may suffer an SPA crash.

  Conditions: This symptom occurs when the CE T1 circuit is configured by the end user for AT&T FDL, and the end user transmits FDL messages requesting 4- hour or 24-hour performance statistics.

  Workaround: There is no workaround. If possible, contact the end user and have them reconfigure their device for ANSI FDL.

- CSCua16786

  Symptoms: When a Cisco 7600 router is placed as a mid-hop-router between the first hop router (FHR) and rendezvous point (RP), with P2P GRE tunnel interface as the FHR facing interface, then PIM-registration might not get completed. The unicast PIM-registration packet might get dropped at the Cisco 7600 router.

  Conditions: This symptom is seen in Cisco IOS Release 12.2(33)SRE6 and RLSx releases.

  Workaround: Delete and create the FHR facing p2p tunnel interface at Cisco 7600 router, which is acting as mid-hop-rtr.

- CSCua17746

  Symptoms: IKEv2 with RSA-Sig as auth session will fail.

  Conditions: The symptom is observed with:

  - IKEv2 + RSA-Sig auth + ISM VPN; or
  - IKEv2 + RSA-Sig auth + 7200 with VSA.

  Workaround: Disable ISM VPN or VSA or do not use IKEv2 RSA-Sig as auth.

- CSCua22599

  Symptoms: MCB timeout error message is seen on console. Ports 7 and 8 do not come up.

  Conditions: This symptom is seen when combo ports come up with media-type.

  Workaround: There is no workaround.

- CSCua30259

  Symptoms: EVC egress traffic does not flow. The frames are dropped by Selene.

  Conditions: This symptom occurs when SPAN is configured on service instance.

  Workaround: There is no workaround.