Bugs for Cisco IOS Release 15.4(2)S

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug.

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results

Note 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:

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

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
Status	Fixed
Severity	2 or higher

Resolved Bugs—Cisco IOS Release 15.4(2)S4

Table 1 Resolved Bugs—Cisco IOS Release 15.4(2)S4

Identifier	Description
CSCuu93699	Crash on IKEv2 cluster hub when anyconnect client tries reconnect
CSCuq46955	IOS ISR AM IKEv1 doesnt work with rsa-sig
CSCus19794	Cisco IOS and IOS XE IPv6 SEND Denial of Service Vulnerability
CSCuu82607	Evaluation of all for OpenSSL June 2015
CSCuq74492	IOS/IOSd Multiple Vulnerabilities in OpenSSL - August 2014
CSCus61884	JANUARY 2015 OpenSSL Vulnerabilities
CSCut46130	MARCH 2015 OpenSSL Vulnerabilities

Resolved Bugs—Cisco IOS Release 15.4(2)S3

Table 2 Resolved Bugs—Cisco IOS Release 15.4(2)S3

Identifier	Description
CSCug18580	ASR1k crash: UNIX-EXT-SIGNAL SEGFAULT, Process = AAA ACCT Proc
CSCur51387	NG3K stack: standby gets reloaded due to reason "configuration mismatch"
CSCur27466	WebUI in IOS-XE : evaluation of SSLv3 POODLE vulnerability
CSCup62315	Autonomic Networking Infrastructure Device Reload DoS Vulnerability
CSCup62191	Autonomic Networking Registration Authority Spoofing Vulnerability
CSCuq35209	BGP advertising incorrect Link Local ipv6 address
CSCuq83441	BGP L2VPN uses default static next-hop instead of outging intf-addr
CSCuq99797	BGP Route-Target not advertised when rtfilter address family in use
CSCuq13985	BGP Router process crash due to recevied BGP withdraw
CSCur66140	Import of Global routes to VRF will fail
CSCuq24984	In rare high BGP update churn case, sh ip bgp x.x.x.x may crash

Identifier	Description
CSCun68322	Support BGP GR for VPN AF in platform without MPLS
CSCuo66933	Switch sent Failure packet after reboot and caused PC to fail authen
CSCus57583	ASR 1K BGP Process Crash Due to EIGRP Route Redistribution
CSCur13495	Service-data of a service change is not updated by SAF forwarder
CSCuq93406	IOSd crash on Ethernet CFM receiving a malformed CFM frame
CSCur43251	POODLE protocol-side fix: HTTPS Client
CSCuo84660	copy command yields DATACORRPUTION error
CSCuq96691	Utah crash during ezconfig installation.
CSCuq17828	ASR: Radius Accounting fails when using EDCSA certs
CSCum90471	ASR1k: Ping failure b/w CE1 & CE3 after Switchover.
CSCus48386	POODLE related fix : LDAPv3 client REQUIRED to support TLS
CSCur36464	mVPN: Inter-AS Option B: Different RDs: proxy vector: local RD is picked
CSCur09682	Router crashes in PIM due to infinite recursion at ip_set_mdb_flag
CSCuq57261	cBR-8 SUP HA Long M-BGP and LDP Resync Delay
CSCur92862	TE leaks memory when restarting isis
CSCul73513	Clock is not matching between server-client after leap configuration
CSCuo29389	NTP clients of 3900 loses sync sporadically,due to high offsetvariations
CSCun62014	Router crash with %SYS-3-BADFREEPTRS after reconfiguring pppoe
CSCut14355	GETVPN - IOS-XE using SW-TCAM - Deny policy classification incorrect
CSCus95855	ISR4451 FMAN-FP Crash
CSCus01735	cbQosTSCfgRate64 is not supported on ASR1k/IOSXE
CSCum87411	software install from tftp get failed fts_client issue
CSCuq41114	ENH: SSH configuration option to restrict cipher public key and HMAC
CSCur23656	Cisco IOS and IOSd in IOS-XE : evaluation of SSLv3 POODLE vulnerability
CSCur44075	AC ICE+ ver <= 4.0 Client unable to connect to XE SSL Headend {CSR1K}
CSCup86552	Issue with qos service installation
CSCuh92882	XE3.11 Seginfo->l2hw_cond_debug is set to "1" when there is no condition
CSCup52725	XE3.13: asr1k RP Crash while 72 hour longevity run
CSCum94811	TCP Packet Memory Leak Vulnerability
CSCup41482	TCP snd window stuck with CEF enabled
CSCuh09324	udp entries not deleted from flowmgr table
CSCus47361	DSMP statistic request timeout cause 4 more seconds to disconnect

Resolved Bugs—Cisco IOS Release 15.4(2)S2

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

Resolved Bugs—Cisco IOS Release 15.4(2)S1

- CSCee32792

  Symptom: A Cisco router reloads at snmp_free_variable_element while using SNMPv3 commands.

  Conditions: This symptom occurs while using SNMPv3 commands.

  Workaround: There is no workaround.

- CSCtz45833

  Symptom: A Cisco router crashes with the following message:

  ```
  Router crash: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = MPLS TE LM
  ```

  Conditions: This symptom occurs when a router acts as the mid point for MPLS-TE tunnels and performs an ERO expansion. In case the ERO expansion fails (due to IGP race conditions or inter-AS scenario) and backup tunnels are in use (for MPLS-TE FRR feature), the router may crash.

  Workaround: Configure the head-ends to perform a full ERO computation to avoid mid points performing any ERO expansion. This can be done using the dynamic path option or by using the explicit path that specifies strict hops for each node along the desired LSP path (using “loose” hops or partial strict hops can lead to this issue).

- 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 bug.

  Workaround: Avoid unconfiguring and reconfiguring BGP L2VPN.

- 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 has been seen while updating various different commands such as, those under “call-manager-fallback” ip route statements interface sub-commands.

  Workaround: There is no workaround.

- CSCug17485

  Symptom: A buffer leak is observed on a Cisco router.

  Conditions: This symptom occurs while using SSLVPN.

  Workaround: There is no workaround.

- CSCug45421

  Symptom: The standby RP crashes.

Conditions: Memory corruption occurs in certain cases when the following commands are executed in quick succession. It leads to a crash later when the memory is accessed. The issue is seen only with on-demand PVCs and when the commands are copied and pasted or executed using a script or tool.

```
configure terminal
interface ATM0/0/0.2 multipoint
range pvc 11/41 11/51
create on-demand
/* Prob commands begin */
pvc-in-range 11/45
exit
no pvc-in-range 11/45
/* Prob commands end */
end
```

Workaround: Do not execute the commands in quick succession.

- CSCuh09324

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

  Conditions: This symptom occurs in the following images

  – ct5760-ipservicesk9.bin
  – cat3k_caa-universalk9.bin
  – cat4500e-universalk9.bin

  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: If you suspect that you are affected by this bug, please do the following, for confirmation:

```
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

- CSCui05000

  Symptom: A Cisco router may crash upon importing a prefix into VRF after applying **no ipv4 multicast multitopology** under "vrf definition" for that VRF.

  Conditions: This symptom occurs while initially configuring the VRF. **address-family ipv4/6 multicast vrf** must be configured under "router bgp" mode before import route-targets are configured under "vrf definition" mode.

  Workaround: There is no workaround.

  More Info: If the crash does not occur, it is likely that importing of the prefix will not work.

- 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.

- 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 configuration).

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

- CSCui59984

  Symptom: REP FLAPs with low LSL timers with the following scale:

  1. Scale of MAC address OR
  2. Scale of Bridge-domain OR
  3. Repeated/multiple REP topology changes OR
  4. CPU-intensive activities.

  Conditions: This symptom occurs with REP configured with low LSL age timer with scale of configuration or any CPU-intensive activities.

  Workaround: Use default LSL timers.

- 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.

- CSCul22914

  Symptom: A Cisco router does not give the necessary failure information if the crypto NIST/KAT tests on boot fail. During test failures, users will not be notified. The logs do not contain information on the failures.

  Conditions: This symptom occurs with a crypto NIST/KAT self test. The message below is a generic message and is not specific to a crypto self test failure.

  ```
  *Nov 5 17:48:19.128: %CMRP-3-CHASSIS_MONITOR_READY_TIME_EXCEEDED:cmand: Reloading F0
  because it has failed to become ready for packet processing
  ```

  This message does not give enough information for the user to take a proper course of action.

  Workaround: There is no workaround.

  More Info: A failure in one of the POST Known Answer Test (KAT) test during boot-up triggers this issue. The issue will not occur if all the KAT tests are passes.

- CSCul24443

  Symptom: A Cisco router crashes while scaling service instances to 3600 whenever the memory is utilized fully and it throws an error as there is no memory to display the output of the **show running** command.

  Conditions: This symptom occurs when the service instance is scaled to 3600.

  Workaround: Reload the router.

- 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.

- CSCul29918

  Symptom: A vulnerability in IPSec tunnel implementation of Cisco IOS Software could allow an unauthenticated, remote attacker to change the tunnel MTU or path MTU and potentially cause IPSec tunnel to drop.

  The vulnerability is due to incorrect processing of certain ICMP packets. An attacker could exploit this vulnerability by sending specific ICMP packets to an affected device in order to change the configured MTU value of the tunnel interface. An exploit could allow the attacker to change the tunnel MTU or path MTU and potentially cause IPSec tunnel to drop.

  Conditions: This symtpom occurs on a device configured for IPSec VTI and with path-mtu-discovery disabled.

  Workaround: The issue is caused by ICMP unreachables. Blocking ICMP is a 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 4.3/4.1:
  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:U/RC:C

  CVE ID CVE-2013-6694 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-2013-6694

  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

- CSCul39964

  Symptom: Sessions do not get cleared. They get stuck in WT_ST state.

  Conditions: This symptom occurs when sessions are closed in bulk mode by shutting any trunk link or during a clear all session from DUT.

  Workaround: There is no workaround.

  More Info: The memory leak issue and WT_ST are related. Along with memory leak, sessions are not cleared on the active RP as they get stuck in WT_ST state.

```
asr1k-1#sh clock
07:18:07.045 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#
asr1k-1#
asr1k-1#sh clock
07:20:08.295 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#
asr1k-1#sh clock
07:46:34.113 CET Thu Nov 14 2013
asr1k-1#su
PTA : Locally terminated sessions
FWDED: Forwarded sessions
TRANS: All other sessions (in transient state)
TOTAL PTA FWDED TRANS
TOTAL 14465 0 6557 7908
GigabitEthernet0/0/0 3024 0 0 3024
GigabitEthernet0/0/1 2587 0 0 2587
GigabitEthernet0/1/0 2297 0 0 2297
GigabitEthernet0/1/1 6557 0 6557 0
asr1k-1#
asr1k-1#s
6557 sessions in FORWARDED (FWDED) State
7908 sessions in WAITING_FOR_STATS (WT_ST) State
14465 sessions totalUniq ID PPPoE RemMAC Port VT
VA State
SID LocMAC VA-st Type
5978 5978 0000.6ca3.0116 Gi0/0/0.2940148 1 Vi2.3091 WT_ST
b414.8901.8e00 VLAN: 294/148 UP
5979 5979 0000.6ca3.0117 Gi0/0/0.2940149 1 Vi2.3092 WT_ST
b414.8901.8e00 VLAN: 294/149 UP
6460 6514 0000.6ca3.0134 Gi0/0/0.2940178 1 Vi2.3354 WT_ST
```

```
b414.8901.8e00 VLAN: 294/178 UP
6454 6508 0000.6ca3.0135 Gi0/0/0.2940179 1 Vi2.3350 WT_ST
b414.8901.8e00 VLAN: 294/179 UP
6453 6507 0000.6ca3.0136 Gi0/0/0.2940180 1 Vi2.3349 WT_ST
b414.8901.8e00 VLAN: 294/180 UP
6518 6572 0000.6ca3.0137 Gi0/0/0.2940181 1 Vi2.3395 WT_ST
b414.8901.8e00 VLAN: 294/181 UP
6514 6568 0000.6ca3.0138 Gi0/0/0.2940182 1 Vi2.3393 WT_ST
b414.8901.8e00 VLAN: 294/182 UP
6516 6570 0000.6ca3.0139 Gi0/0/0.2940183 1 Vi2.3394 WT_ST
b414.8901.8e00 VLAN: 294/183 UP
6560 6614 0000.6ca3.013a Gi0/0/0.2940184 1 Vi2.3413 WT_ST
```

- 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.

- CSCul94606

  Symptom: Standby CUBE crashes while handling an agent transfer.

  Conditions: This symptom is observed when an agent transfers the call to another agent.

  Workaround: There is no workaround.

- CSCum09990

  Symptom: Basic mgcp t38-fax call fails between T1/cas endpoints as call not getting confirmed at terminating end.

  Conditions: This symptom occurs on Cisco 2900 routers which have been booted with Cisco IOS Release 15.4(1.14)T images.

  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.

- CSCum20647

  Symptom: A traceback is seen in fn_resiliency_phase2 Script Cisco XE3.12/PI24 Release.

Conditions: A traceback is seen in fn_resiliency_phase2 Script Cisco XE3.12/PI24 Release. Functionality test is going fine but test fail when routers health check is done during cleanup.

Workaround: There is no workaround.

More Info: The issue seen only when GETVPN group is removed.

- CSCum33167

  Symptom: When PPPoE-IA is enabled, a Cisco switch forwards PADR/PADT packets to an untrusted port.

  Conditions: This symptoms occurs under the following conditions:

  – Configure PPPoE IA globally on node 1.
  – Configure service instance on interface gig0/1,gig 0/2 and gig 0/3.
  – Configure PPPoE IA on the interface and on the service instance.
  – Configure gig 0/1 and gig 0/3 as an untrusted port and gig 0/2 as a trusted port.
  – Send a PADI Packet from client 1 and send a PADO packet from the server.

  The PADO packet is received on client 2, but it should be received only on client 1. Send a PADR packet from client 1, client 2 also receives the packet. But it should not receive the packet. The PADR/PADT packet should be forwarded only to a trusted port.

  Workaround: There is no workaround.

- CSCum40306

  Symptom: A Cisco router crashes during call transfer in SRST mode.

  Conditions: This symptom is observed during call transfer in SRST mode, including SCCP phones.

  Workaround: There is no workaround.

- CSCum48221

  Symptom: 3560CG box memory is showing as low as 3.15MB.

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

  Workaround: There is no workaround.

- CSCum52216

  Symptom: After a reload, **ip pim sparse-mode** is gone on interface lisp 0.x (x denoted the LSIP interface number).

  Conditions: This symptom occurs after a reload.

  Workaround: There is no workaround.

- CSCum60848

  Symptom: Under certain conditions, a DSP will hang in certain call scenarios including REFER passthrough.

  Conditions: This symptom is observed under heavy load.

  Workaround: There is no workaround.

- 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.

- CSCum62783

  Symptom: The following alignment errors are seen after a PPPoE session establishment for the first time after a reboot:

  ```
  *Jan 14 07:24:40.591: %ALIGN-3-CORRECT: Alignment correction made at 0x32B2DFF4z
  reading 0xE7790ED *Jan 14 07:24:40.591: %ALIGN-3-TRACE: -Traceback= 0x32B2DFF4z
  0x32B1E274z 0x32B1EECCz 0x32B1EF90z 0x332E550Cz 0x332E54F0z 0xFFFF1A00z 0xFFFF1A00z
  ```

  Conditions: This symptom occurs when **pppoe-client ppp-max-payload** is configured under the Ethernet interface.

  Workaround: There is no workaround.

- CSCum66102

  Symptom: A Cisco router may crash when the CLI i**p nbar custom** <*name*> <*byte-offset*> **ascii** <*pattern*> **tcp** <*port*> is used. The crash occurs only when the ascii flavor of the **ip nbar custom** command is used.

  Conditions: This symptom is not observed under any specific conditions. It occurs on all types of ASR and ISR-G2 routrs as well as on 7200.

  Workaround: Avoid using the ascii flavor of the **ip nbar custom** command (Example: i**p nbar custom** <*name*> <*byte-offset*> **ascii**)

- CSCum67229

  Symptom: Entitymib does not respond for OC3/OC12/T3/E3 controller ports on the Cisco ME3600x-24CX-M platform.

  Conditions: This symptom occurs with the Cisco ME 3600X-24CX-M platform running Cisco IOS XE Release 3.10.

  Workaround: There is no workaround.

- CSCum81041

  Symptom: One way audio incoming calls redirected through CVP.

  Conditions: Call flow: ----------

  ```
  Caller----G711----TDM GW----SIP-----ASR1K----SIP-----CUSP----SIP----CVP(Vz0)----IP-IVR
  | | -----SIP---CVP (BAMS) | |--------SIP---CUCM---Agent Phone (G729 only)
  ```

  Initially the caller is connected to IP-IVR, both ingress and egress leg of the CUBE is doing G711. Call is connected to the IP-IVR, then CVP sends a refer to the VXML GW for playing prompts and ringback tone etc. When the call is transferred to the agent, CUBE negotiated G729 at the sip level with the CVP, but because of mid-call signaling block on the ingress side, continue with the G711. Hence xcoder is invoked on the CUBE to handle G729 to G711 and vise versa, but CUBE is still sending G711 media to the agent phone side while the agent phone is sending G729 media to the CUBE.

  Workaround: There is no workaround.

- CSCum84999

  Symptom: SUBSCRIBE received from CVP after BYE and NOTIFY with subscription-state : terminates is send by CUBE.

  Conditions: This symptom is observed when SUBSCRIBE IS received after call is terminated with BYE.

Workaround: There is no workaround.

- CSCum85493

  Symptom: Ping fails with tunnel protection applied.

  Conditions: Tunnel protection applied on GRE tunnel interface, using IKEv1 to negotiate IPsec SAs and remote node (IKEv1 responder) behind NAT.

  Workaround: The users can switch to IKEv2.

- 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.

- CSCum94228

  Symptom: Local CAC displaying all information about each flows. This may impact show output for customer in a set up where we could possibly have large number of flows.

  Conditions: This symptom is observed in a scaled configuration.

  Workaround: There is no workaround.

- CSCum95078

  Symptom: Large IPSEC packets get dropped when fragmentation is done after IPSEC encapsulation.

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

  Workaround: There is no workaround.

- 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.

- CSCun02605

  Symptom: ASR crashes with no known trigger in CCSIP_SPI_CONTROL process.

  Conditions: It is an error scenario where crash occurs when router is not able to send ACK for 200 OK where branch parameters differ.

```
CUBE INVITE | INVITE (Via branch=ABC) ----------------------------->|
---------------------------------------> | 200 OK (Via branch=DEF) |
<---------------------------------------- |
```

  Cube fails to send ACK to 200 OK for some reason and causes a crash

  Workaround: There is no workaround.

- CSCun07843

  Symptom: A critical alarm is observed on the FPGA port 0/5/0.

  Conditions: This symptom occurs after performing an SSO.

  Workaround: There is no workaround.

- 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.

- CSCun21602

  Symptom: Traffic is not forwarded by the router out of any interface.

  Conditions: This symptom occurs on toggling of the **ip routing** command in global configuration mode.

  Workaround: Perform shut and no shut of the interface which is involved in forwarding or reload the device with **ip routing** enabled.

- 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: This symptom occurs on a 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

- CSCun31359

  Symptom: Memory corruption crash while processing the sip-profile rule.

  Conditions: This symptom occurs on a Cisco 3900 device running Cisco IOS Release 15.3(1)T.

  Workaround: Perform the following workaround:

  – Using history-info pass-through feature (voice service voip -> sip -> history-info)

  – Using header pass-through feature

- CSCun31450

  Symptom: CPU hog followed by crash.

  Platforms affected are:

  – ct5760-ipservices.bin

  – cat3k_caa-universalk9.bin

  – cat4500e-universalk9.bin

  Conditions: This issue occurs while running udp IP SLA applications.

  Workaround: There is no workaround.

- 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.

- CSCun35070

  Symptom: Targeted LDP sessions between Customer Edge devices will flap every 3 minutes. IGP, Interface LDP between CE devices will run fine.

  Conditions: This symptom occurs when an MPLS LDP packet is carried over an L2VPN cloud with the control word OFF.

  Workaround: Configure the control word ON in an L2VPN cloud.

- CSCun36655

  Symptom: If the terminal adjacency of a lisp interface is removed and then re-added, the lisp interface MTU may remain at the invalid value of 65535. This can be seen in the **show cef interface** <*intf*> **internal** command output.

  IPsec will obtain the MTU value from CEF and LISP, and the incorrect MTU will cause drops of large packets.

IPSEC MTU incorrectly computed - causing packet drops on large packets traversing from “inside” to “outside” are dropped.

Conditions: This symptom is observed in the following Cisco C800 Series:

Cisco IOS Software, C890 Software (C890-UNIVERSALK9-M), Version 15.3(3)XB12, RELEASE SOFTWARE (fc2)

Workaround: A workaround is to toggle the IP MTU config on the lisp interface. Use “show run lisp0.1” to determine the MTU. Then use “ip mtu <mtu>” to first set it to a lower value, and then to set it back to the original value.

```
Example:
sh run interface lisp0.1
interface LISP0.1
ip mtu 1398
crypto map CM
end

conf t
interface lisp0.1
ip mtu 1200
ip mtu 1398
```

More Info: Originally [Cisco IOS Release 15.3(1)T] the MTU was accurately computed as:

```
RTR13-xTR#sh cry ipse sa vrf DeptA | in mtu
    path mtu 1456, ip mtu 1456, ip mtu idb LISP0.1
    path mtu 1456, ip mtu 1456, ip mtu idb LISP0.1
    path mtu 1456, ipv6 mtu 1456, ipv6 mtu idb LISP0.1
    path mtu 1456, ipv6 mtu 1456, ipv6 mtu idb LISP0.1
RTR13-xTR#
```

In 153-3.XB12, the MTU is as follows:

```
!RTR#show crypto ipsec sa | inc mtu
!     plaintext mtu 65458, path mtu 65535, ip mtu 65535, ip mtu idb LISP0
```

- CSCun36866

  Symptom: A Cisco router providing Layer 2 EoMPLS services may stop forwarding ingress and egress traffic for an xconnect for which a backup peer configuration has been applied.

  Conditions: This symptom occurs in Cisco 7600 Series routers and Cisco ASR 1000 Series routers running Cisco IOS Release 15.3(3)S or 15.4(02)S with xconnect configured under a service instance.

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

- CSCun41292

  Symptom: On a Cisco ASR 1001 router running Cisco IOS Release 15.3(1)S, a crash occurs when the “show ip ei vrf X topo X.X.X.X/X” command is executed. The X.X.X.X/X must be in “FD is infinity” status in EIGRP as CSCtz01338.

```
asr1001_bew_03# show ip ei vrf * to all |
i Infinity P 174.162.XX.XX/24, 0 successors, FD is Infinity, U, serno 37, refcount 1
snip P 174.180.XX.XX/29, 0 successors, FD is Infinity, U, serno 46, refcount 1
asr1001_bew_03#show ip ei vrf 1 to 174.162.XX.XX/24
Exception to IOS Thread: Frame pointer 0x7F63DF6602D0, PC = 0x1956C8D
UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Exec -Traceback=
1#980611ad3b9665cd80fe5178bcd6036a :400000+1556C8D :400000+1556B09 :400000+15569D1
:400000+157DE39 :400000+15197A2 :400000+1518659 :400000+156BA5E :400000+15591D1
:400000+1189768 :400000+1188E6D :400000+1186E15 :400000+484F270 :400000+11A1CA0
```

```
Fastpath Thread backtrace: -Traceback= 1#980611ad3b9665cd80fe5178bcd6036a
c:7F64154A4000+BE002
Auxiliary Thread backtrace: -Traceback= 1#980611ad3b9665cd80fe5178bcd6036a
pthread:7F640ED43000+A7C9
```

Conditions: This symptom occurs when X.X.X.X/X is in “FD is infinity” status in EIGRP.

Workaround: There is no workaround.

- CSCun45272

  Symptom:

  1. Standby RP will have out-of-sync entries. With MPLS-TE NSR enabled, the standby RP will have out-of-sync entries which will result in flapping of the path-protected LSP of the tunnel after an SSO.
  2. Leaking an LSP. A third LSP will be signaled and leaked (there is no management of the LSP). There are supposed to be two LSPs at steady state (primary and path protected), but with this defect, there will be primary, path protected, and leaked LSP.

  Conditions: This symptom occurs with a reoptimization of a tunnel that has failed with path protection enabled.

  Workaround: There is no workaround.

- CSCun45299

  Symptom: IPv6 traffic is dropped for packets with extension headers.

  Conditions: This symptom occurs when extension header packets are punted to the CPU.

  Workaround: There is no workaround.

- CSCun46486

  Symptom: A Cisco device crashes every 2-3 days when the SNMPSET operation is used to create guest users.

  Conditions: This symptom occurs when guest users are created through SNMPSET operations at a very high rate.

  Workaround: There is no workaround.

- CSCun47357

  Symptom: Enabling PBR breaks the EIGRP multicast.

  Conditions: This symptom occurs under the following conditions:

  1. Create a route map for any random IP address (not necessarily related to multicast/protocol IP).
  2. Enable the PBR on an interface with EIGRP peering. It is observed that the EIGRP peering goes down.

  Workaround: There is no workaround.

- CSCun47461

  Symptom: A crash occurs on issuing the **no switchport** command on an interface applied with a MAC ACL.

  Conditions: This symptom occurs on issuing the **no switchport** command on an interface applied with a MAC ACL.

  Workaround: There is no workaround.

- 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.

- CSCun50243

  Symptom: When CED/ANSam/2100Hz answer tone is detected in the early media phase of the call, the gateway does not switchover and starts sending distorted audio to the originating fax. Fax transmission fails.

  Conditions: This symptom is observed when modem passthrough nse codec g711ulaw is used as the fax protocol.

  ```
  Fax -> VG224 --SCCP--> CUCM -SIP--> 3945 GW--ISDN T1 PRI-->PSTN 3945 IOS: 15.1.4M5
  VG224:15.1.4M2
  ```

  Workaround: Perform the following workaround:

  – Use “progress_ind” to strip PI=8 if the Early Media is opened via an ISDN ALERTING message: (config-dial-peer)#progress_ind alert strip

  – Check with Carrier if they can avoid opening early media for Fax/Modem calls.

  – More Info: Early media cut-through for fax/modem calls is not supported. The expected flow transition to the Voice Band Data (VBD) mode or modem up-speed as we commonly call it,requires a VoIP call to be first established (call is connected). It is then, when normally a 2100Hz answer tone is detected as the media flows in both direction and triggers Voice Band Data (VBD) upspeed.

- CSCun58030

  Symptom: A Cisco ME3600-24CX platform does not display time source information while running the PTP dataset time properties show command. Functional issues are not noticed with PTP time sync. The time source field says “Unknown”.

  Conditions: This symptom does not occur under specific conditions. A simple Ordinary Clock(OC) Slave- Master connectivity would make the Slave show up as “Time Source Unknown”.

  Workaround: There is no workaround.

- CSCun58224

  Symptom: A memory corruption is observed on scaling NAT sessions.

  Conditions: This symptom occurs due to multiple translation entries of NAT with overload.

  Workaround: There is no workaround.

- CSCun62420

  Symptom: Any ingress policy on an EFP affects other EFPs on the same physical port with local-connect configuration.

  Conditions: This symptom occurs when an ingress QoS policy is enabled on an EFP and another EFP of the same port is bound to the other port’s EFP by the “connect” statement.

  Workaround:

  1. Apply an ingress policy on all EFPs with a local-connect configuration and detach the policy.
  2. Configure an independent service-policy on the erroneously affected EFPs of the same physical interface.

- CSCun65000

  Symptom: Traffic loss of about 200-500 ms is observed.

  Conditions: This symptom is observed on an RLFA cutover.

  Workaround: There is no workaround.

- CSCun65380

  Symptom: CME Crashed while Inbound SIP profile added globally.

  Conditions: This symptom is observed when inbound SIP profile is added.

  Workaround: Do not configure inbound sip profile.

- CSCun67364

  Symptom: Convergence on Local link failure with rLFA is higher than one second.

  Conditions: Configure rLFA and perform local link failure. The problem is likely seen when configuring a small spf-interval value.

  Workaround: Do not configure too small spf-interval.

- CSCun68723

  Symptom: Incorrect information is present on the E1/T1 ports on the Cisco ME 3600X 24CX platform in the IfTable of IF-MIB.

  The incorrect information includes the following:

  1. ifType of the interface is 0 which is not a valid ifType.
  2. ifAdminStatus value is always testing, and does not reflect the actual state.
  3. ifOperStatus value is always unknown and does not reflect the actual state.
  4. ifSpeed value is 0 which is incorrect.

  Conditions: This symptom occurs on any Cisco ME 3600X 24CX device running Cisco IOS Release 15.3(3)S.

  Workaround: The correct information on the E1/T1 ports is available in CLI.

- CSCun72459

  Symptom: High traffic loss is observed with setups having BGP and microloop avoidance combination.

  Conditions: This symptom occurs with the following combination:

  1. IP FRR is turned on.
  2. Cisco IOS XE Release 3.11 code (or newer) that enables microloop avoidance by default.
  3. BGP configurations.

  Workaround: Disable the microloop avoidance feature. For example, in ISIS, execute the following commands:

  router isis <process name>

  microloop avoidance disable

  !

  However, there will be some traffic loss due to the lack of microloop avoidance.

- CSCun72939

  Symptom: QoS Egress Marking does not work for GRE Tunnels.

Conditions: This symptom is observed under the following conditions: -The issue happens for fragmented packet. -The issue is found on Cisco IOS Release 15.3(3)M2.

Workaround: There is no workaround.

- CSCun73782

  Symptom:

  A vulnerability in LISP control messages processing on Cisco IOS and Cisco IOS XE could allow an unauthenticated, remote attacker to cause a vulnerable device to disable CEF forwarding and eventually drop traffic passing through.

  The vulnerability is due to insufficient checking of certain parameters in LISP control messages on ITR. An attacker could exploit this vulnerability by sending malformed LISP control messages to ITR. An exploit could allow the attacker to cause a vulnerable device to disable CEF forwarding and eventually drop traffic passing through.

  Conditions: Malformed messages can only be generated by a device that is already registered to a LISP system: a valid ETR or ALT.

  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-2014-3262 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-2014-3262

  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

- CSCun75719

  Symptom: After a switchover, standby device crashes with traceback.

  Conditions: At present, this is observed only on advipservices images in mtrose branches.

  Workaround: There is no workaround.

- CSCun76733

  Symptom: BFD goes down and remains in Admindown state.

  Conditions: This symptom occurs after applying ACL chaining and flapping of the interface.

  Workaround: There is no workaround.

  More Info: An IPv4 BFD neighbor remains in admindown state on the PE. The ACE configured in ACL for BFD is matched and the receive counters on BFD neighbors are incremented but the BFD is still down.

  This issue occurs only after ACL chaining is applied.

- 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.

- CSCun78309

  Symptom: An Mroute entry on FHR is stuck in a registering state in MVPNv4.

  ```
  show ip mroute vrf <vpn-name> -->> shows the mroute entry in registering state
  ```

  Conditions: This symptom occurs when the source address of the encapsulation tunnel for PIM registers on the FHR is one of the interfaces that is not in the same VRF as the register tunnel itself.

  Workaround: There is no workaround.

  More Info: sample Output:

  ```
  ----------------------

  PE2#show ip mroute vrf vpn1
  (215.12.1.2, 229.40.1.1), 00:00:29/00:02:30, flags: FT Incoming interface:
  GigabitEthernet3/3.1, RPF nbr 0.0.0.0, Registering Outgoing interface list: Tunnel764,
  Forward/Sparse, 00:00:29/00:03:00
  ```

- CSCun81754

  Symptom: snmpEngineBoots integer does not increment on Cisco ME 3800 and Cisco ME 3600 devices once they are reloaded. They get reinitialized.

  Conditions: This symptom occurs only when the device gets rebooted. A warm restart increases the value.

  Workaround: There is no workaround.

- CSCun85501

  Symptom: IPv6 traffic is not forwarded in the hardware for templates other than default and video (like VPNv4-only, VPNv4-v6). However, IPv4 traffic works fine.

  Conditions: This symptom occurs when the template is not default or not video

  Workaround: There is no workaround.

  Further Problem Description: IPv6 traffic is punted to the CPU.

- CSCun87557

  Symptom: A Cisco router crashes.

  Conditions: This symptom occurs when the VTY Service Set maximum response is set to a small number, for example, 10, and then multiple commands are sent separated by a newline using the same write, for example, “show ver\nshow ver\n”.

  Workaround: Set the maximum response to a bigger number.

- CSCun91720

  Symptom: IPv6 mcast traffic is punted to the host queue (inl3idc_vlan.bridgeBasedMcastIp=1).

  Conditions: This symptom occurs on a Layer 2 device with no multicast configurations.

  Workaround: There is no workaround.

  More Info: Instead of bridging the IPv6 traffic, the switch punts it to the CPU.

- CSCun91923

  Symptom: Router crash observed on CUBE for Carbon2-SIP signaling forking.

  Conditions: Crash is seen while you configure CUBE for SIP signaling forking on PI19.

  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: This symptom occurs when the 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 <>”.

- CSCuo09249

  Symptom: An xTR changes its RLOC, map-request packets from that new RLOC are dropped on the MS/MR due to policy violation, for example:

  ```
  *Apr 2 15:29:15 JST: LISP-0: AF IID 100 IPv4, Map resolver filtered incoming map
  request from 2400:A:A:9999:C267:AFFF:FE52:287 because it does not conform to the
  configured allowed-locator policy.
  ```

  Conditions: This symptom is observed when {ipv4|ipv6} map-resolver map-request validate source registered is configured on the MS/MR and the xTR RLOC is updated, for example, by DHCP when the {ipv4|ipv6}-interface configuration is used in the database-mapping configuration. Both the new and the old RLOC must have been valid.

  Workaround: Remove and re-add database-mapping configuration on xTR, possibly using EEM script on address change Remove “{ipv4|ipv6} map-resolver map-request validate source registered” configuration on MS/MR clear lisp site <name> on the MS

- CSCuo11238

  Symptom: Router crashes when removing address-family from VRF definition, or when removing the VRF definition.

  Conditions: This symptom is observed when PIM is configured for the LISP interface associated with the VRF.

  Workaround: Unconfigure LISP for the VRF, or remove PIM configuration from the LISP interface associated with the VRF, before removing VRF configuration.

- CSCuo11703

  Symptom: The **show network-clock synchronization** command flaps between different QL values on the same interface. Depending on the values with which the interface flaps, this could lead to triggering of network-clock selection algorithm and subsequent selection of primary reference clock for the system.

  Conditions: This symptom could occur when the network-clock synchronization mode is unprovisioned from automatic selection, and then the monitor interfaces are removed and a new set of interfaces are added for network-clock monitoring with automatic selection reprovisioned.

  Workaround: Adding back the older set of interfaces and removing them would resolve the issue.

- CSCuo12245

  Symptom: The following error message is observed with traceback:

  ```
  OCE_PUNT_PROCESS-3-LABEL_CACHE_INVALID: inlabel pointer was NULL
  ```

  Conditions: Multicast traffic is label switched in the mpls P2MP tree and replicated at branch bud nodes along the P2MP tree. The error condition is observed at a bud node, where the replicated traffic is dropped with the error.

  Workaround: There is no workaround.

- 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.

- 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”.

- CSCuo19730

  Symptom: Cisco IOS XE includes a version of OpenSSL that is affected by the vulnerability identified by the Common Vulnerability and Exposures (CVE) ID CVE-2014-0160.

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

  Conditions: Cisco IOS XE devices running release 3.11.0S, 3.11.1S or 3.12.0S and with the WebUI interface over HTTPs enabled. No other versions of Cisco IOS XE are affected.

  Devices with the WebUI interface enabled and using HTTPs as transport protocol will include the following configuration:

  transport-map type persistent webui http-webui secure-server ip http secure-server transport type persistent webui input http-webui

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S but WITHOUT the WebUI interface enabled, or with the WebUI interface enabled but NOT using HTTPs as transport protocol are NOT AFFECTED by this vulnerability.

  Devices running IOS XE release 3.11.0S, 3.11.1S or 3.12.0S and with the HTTPs server enabled (by including in their configuration the line “ip http secure-server”) are NOT affected. Both the HTTPs server and the WebUI interface need to be enabled for a device to be vulnerable.

  The WebUI configuration guide is available at http://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asrswcfg/webui.html

  Workaround: Not currently available.

  Further Problem Description: Additional details about this vulnerability can be found at http://cve.mitre.org/cve/cve.html

  Software version and Fixes:

  The first column is the Cisco IOS XE Software Release.

  The second column is the First Fixed Release.

  2.x.x Not Vulnerable

  3.1.xS Not Vulnerable

  3.1.xSG Not Vulnerable

  3.2.xS Not Vulnerable

  3.2xSE Not Vulnerable

  3.2.xSG Not Vulnerable

  3.2.xXO Not Vulnerable

  3.2.xSQ Not Vulnerable

3.3.xS Not Vulnerable

3.3.xSE Not Vulnerable

3.3xSG Not Vulnerable

3.3xXO Not Vulnerable

3.3xSQ Not Vulnerable

3.4.xS Not Vulnerable

3.4.xSG Not Vulnerable

3.5.xS Not Vulnerable

3.5.xE Not Vulnerable

3.6.xS Not Vulnerable

3.6.xE Not Vulnerable

3.7.xS Not Vulnerable

3.8.xS Not Vulnerable

3.9.xS Not Vulnerable

3.10.xS Not Vulnerable

3.11.xS Vulnerable

3.12.xS Vulnerable

3.12.0aS Not Vulnerable

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 4.3/4.3:

https://intellishield.cisco.com/security/alertmanager/cvss?target=new&version=2.0&vector=AV:N/AC:M/Au:N/C:P/I:N/A:N/E:H/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.

CVE-2014-0160 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/web/about/security/psirt/security_vulnerability_policy.html

- 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.

- CSCuo24235

  Symptom: SVI counters are not updated for IPv6 traffic.

  Conditions: This symptom does not occur under specific conditions.

  Workaround: There is no workaround.

- CSCuo35867

  Symptom:

  1. CPOS-based PPP serial interface is UP/DOWN; but HDLC is UP/UP; loopback local for PPP is also UP/DOWN;
  2. From debug, the following output is seen:

```
*Apr 16 20:46:50.330: AAA/ID(00100066): PPP allocated .... *Apr 16 20:46:50.831: CCM:
Failed to create session, session already exists <<<<<<<<<<<< *Apr 16 20:46:50.831:
AAA/ID(NA): PPP allocating *Apr 16 20:46:50.831: CCM GROUP:ERROR group not found with
shdb 0 *Apr 16 20:46:50.831: AAA/ID(NA): propagate hw:Se1/0/0.1/1/6/1:0,0x42352E64
sw:Se1/0/0.1/1/6/1:0,0x42353C48 other:nil base:nil unit:0/1 slot:1 shelf:0 tty:nil
*Apr 16 20:46:50.831: aaa_uid_propogate grabbed_id = 1048678 *Apr 16 20:46:50.831:
AAA/ID(00100066): PPP allocated *Apr 16 20:46:52.847: Se1/0/0.1/1/6/1:0 PPP: Missed a
Link-Up transition, starting PPP <<<<<<<<<<<<<
```

  Conditions: This symptom occurs with PPP serial interface flapping.

  Workaround: Chassis reload can temporarily make PPP interface UP/UP, but the problem will reoccur after a few days.

- CSCuo46609

  Symptom: A router configured as an SSL VPN hub may experience a crash due to memory corruption in the I/O pool. The following may be observed in the crashinfo file:

```
<i>validblock_diagnose, code = 1
current memory block, bp = 0xC020750, memorypool type is I/O data check, ptr =
0xC020780
next memory block, bp = 0xC020890, memorypool type is I/O data check, ptr = 0xC0208C0
previous memory block, bp = 0xC020610, memorypool type is I/O data check, ptr =
0xC020640
<memory dump omitted>
Apr 24 13:32:27.860: %SYS-3-OVERRUN: Block overrun at C020750 (red zone 75F405A7)
-Traceback= 60213FD4z 60217688z 649D8D98z 649D54A0z 63C66204z 63C661E8z Apr 24
13:32:27.860: %SYS-6-MTRACE: mallocfree: addr, pc 52E00584,63462AA0 52E00584,63462670
52E00584,30000012 5266D34C,62E3E0B8 52670418,62E3E0B8 53A44BE0,60000284
53A444CC,626CF044 50B6BC0C,62E63294 Apr 24 13:32:27.860: %SYS-6-MTRACE: mallocfree:
addr, pc 5310B904,62E23040 50B6BC0C,62E58E78 50B6BC0C,3000002E 53A45014,6000006A
53A44BE0,64C7A348 53A44BE0,64C79E10 53A44BE0,40000202 53929890,60000266 Apr 24
13:32:27.860: %SYS-6-BLKINFO: Corrupted redzone blk C020750, words 136, alloc
602191F4, InUse, dealloc A2A4170, rfcnt 1 -Traceback= 64049030z 60213FD4z 60217688z
649D8D98z 649D54A0z 63C66204z 63C661E8z Apr 24 13:32:27.864: %SYS-6-MEMDUMP:
0xC020750: 0xAB1234CD 0xFFFE0000 0x0 0x6500240C Apr 24 13:32:27.864: %SYS-6-MEMDUMP:
0xC020760: 0x602191F4 0xC020890 0xC020624 0x80000088 Apr 24 13:32:27.864:
%SYS-6-MEMDUMP: 0xC020770: 0x1 0x0 0x1000001 0x682757A8
%Software-forced reload
14:32:27 SUMMER Thu Apr 24 2014: Breakpoint exception, CPU signal 23, PC =
0x6064C738</i>
```

  Conditions: This has been observed on the following conditions:

  1. 7200 router running Cisco IOS Release 15.2(4)M2 and 15.3(3)M2.
  2. Router is configured as an SSL VPN host.

Workaround: There is no workaround at this time.

- CSCuo47380

  Symptom: Traffic drops in the MST region during IM-OIR followed by an SSO. When an IM is removed from the router, the MST states are not reflected in the standby RSP. If a switchover happens at this state, it could cause total traffic drop.

  Conditions: This symptom is seen in HA routers. If this issue is hit, the IM that was previously removed should not be inserted back, as it could cause a traffic loop.

  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.

- 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.

- CSCuo55180

  Symptom: A vulnerability in PPPoE processing code of Cisco IOS XE could allow an unauthenticated, adjacent attacker to cause a reload of the affected device and eventually a denial of service (DoS) condition.

  The vulnerability is due to improper processing of certain malformed PPPoE packets. An attacker could exploit this vulnerability by sending a malformed PPPoE packet to an IOS XE ASR1000 device, configured with PPPoE termination. An exploit could allow the attacker to cause a reload of the affected device and eventually a denial of service (DoS) condition.

  Conditions: Cisco ASR 1000 with IOS XE, configured for PPPoE termination.

  Workaround: There is no workaround.

  Further Problem Description: A device crashing, may print the following messages on the console:

  ```
  %SYS-3-OVERRUN: Block overrun at 7F7FAE750B58 (red zone 44534C5F00000000)
  %SYS-6-MTRACE: mallocfree: addr, pc ? %SYS-6-BLKINFO: Corrupted redzone blk
  7F7FAE750B58, words 404, alloc 6374D1B, InUse, dealloc 10001, rfcnt 1 ?
  %Software-forced reload
  Exception to IOS Thread: Frame pointer 0x7F7FA0AB5AD8, PC = 0x7F80A8469565
  UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps -Traceback=
  1#c3a5522ccb47820b036322d6b7226e1c c:7F80A8438000+31565
  ```

```
Fastpath Thread backtrace: -Traceback= 1#c3a5522ccb47820b036322d6b7226e1c
c:7F80A8438000+BDDD2
Auxiliary Thread backtrace: -Traceback= 1#c3a5522ccb47820b036322d6b7226e1c
pthread:7F80A3697000+A7C9
```

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:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2014-3284 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-2014-3284

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

- CSCuo55440

  Symptom: The ME3600-24CX device crashes whenever it is reloaded.

  Conditions: This symptom occurs when the ME3600-24CX device is reloaded.

  Workaround: There is no workaround.

- CSCuo56173

  Symptom: When PW's remote peer is ALU, it takes 5 to 10 minutes for the PWs to come up.

  Conditions: This symptom occurs when Provision PW is done first on the ALU and then on the Cisco router.

  Workaround: Provision PW on the Cisco router first.

- CSCuo72301

  Symptom: Crash occurs when IKEv2 attempts to clean up its contexts when it times-out waiting for received Certificate to be Validated by PKI component.

  Conditions: Authentication with certificates and PKI component's response to certificate validation is delayed.

  Workaround: There is no workaround.

- CSCuo77574

  Symptom: An error is seen while enabling "auto negotiation".

  Conditions: This symptom is observed when "auto negotiation" is configured on an interface.

  Workaround: There is no workaround.

- CSCuo82355

  Symptom: A BFD session fails to come up.

  Conditions: This symptom occurs when BFD is running on Cisco IOS Release 15.4(1)S to any other lower release.

  Workaround: Upgrade the device.

- CSCuo86424

  Symptom: An ESP crashes while using packet-trace to debug packets.

  Conditions: This symptom occurs when a ping is initiated while using packet-trace to debug packets on Cisco IOS XE Release 3.11.2 or Cisco IOS Release 15.4(2)S2. This issue is only visible in the Cisco IOS Release 15.4(1)S2 maintenance release.

Workaround: Use packet-trace in a circular mode and choose a large number of packets.

```
Example: debug platform packet-trace packet 8192 circular
```

This will only reduce the chances of seeing the crash but will not eliminate it completely.

- 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: This symptom occurs in 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: None currently available.

  Further Problem Description: 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

Open Bugs—Cisco IOS Release 15.4(2)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.4(2)S. All the bugs listed in this section are open in Cisco IOS Release 15.4(2)S. This section describes only severity 1, severity 2, and select severity 3 bugs.

- CSCum90044

  Symptom: FRR database value does not exist.

  Conditions: This symptom occurs on tunnelling intf with Auto-Tunnel_Primary_SSO_Configuration.

Workaround: There is no workaround.

Resolved Bugs—Cisco IOS Release 15.4(2)S

- CSCtb34814

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

  Conditions: This issue occurs under normal conditions.

  Workaround: There is no workaround.

- CSCte77398

  Symptom: A Cisco ATM router configured with ATM PVC Range commands report the following error when attempting to configure a PVC Range:

  ```
  Unable to configure PVC Range. Possibly multiple users configuring IOS simultaneously.
  ```

  Conditions: This problem occurs randomly and even if there are no multiple sessions accessing the pvc-range at the same time.

  Workaround: There is no workaround.

- CSCts14036

  Symptom: Memory “Holding” continues to increases on process “IP SNMP”. This could lead to an out of memory crash.

  Conditions: This symptom only affects Cisco IOS release 12.2(53)SG5, under the following conditions:

  1. Switch is configured to receive informs

  and/or

  2. Traps received and consumed by switch (traps broadcast)

  Use “show proc memory | inc IP SNMP” and compare outputs across several collections of this command.

  Workaround: Upgrade to Cisco IOS release 12.2(53)SG8.

- CSCty92208

  Symptom: A crash is seen on the Cisco Catalyst 6509 Switch after configuring WCCP.

  Conditions: This symptom occurs when WCCP is configured with a hash assignment and port hashing is enabled. It will occur during redirection if packets are software switched.

  Workaround:

  1. Disable port-hashing if hash-assignment is used.
  2. Use the mask-assignment method.

- 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.

- CSCuc24927

  Symptom: A segmentation fault is seen when IMA, CEM and Serial are configured on different controllers and an image is loaded.

  Conditions: This symptom is seen when IMA, CEM, and Serial are configured on different controllers. and try to load image. The issue is consistently reproduced and is sometimes seen when CEM on TDM and MLPPP QoS on OC3 IM is configured and multiple reloads are done. When there is a segmentation fault, the RSP will not come up and will go to the ROMmon mode.

  Workaround: Do not combine IMA, CEM and Serial configurations. Test each feature individually.

- 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 signalling are affected by this bug.

  Workaround: Avoid unconfiguring and reconfiguring BGP L2VPN.

- CSCue59450

  Symptom: IOS XE Watchdog message seen along with RP and SIP crash.

  Conditions: This symptom is observed in an ARP request on the interface having VRF receive configured on it.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCuh44420

  Symptom: When a Cisco IOS router with one or more mpls ldp neighbors undergoes an **mpls ldp router-id** configuration change and non-stop routing had been previously enabled and disabled prior to the router-id configuration change, sessions fail to become NSR-ready once **mpls ldp nsr** is reconfigured.

  Conditions: This symptom occurs when the **mpls ldp router-id** command is reconfigured after **mpls ldp nsr** has been enabled and then disabled. After the router-id change, **mpls ldp nsr** must be reconfigured in order to encounter this issue.

  Workaround: Reload the standby RP.

- 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.

- CSCuh89168

  Symptom: The standby resets in a continuous loop.

  Conditions: This symptom occurs on insertion of a new standby RSP with a different license than the one on the active RSP.

  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.

- 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.

- CSCui11998

  Symptom: A CEM-SSO Standy crash occurs with 576 CEMoMPLS configured on the mobile profile testbed after defaulting the CEM interface configuration and during reconfiguration.

  Conditions: This symptom occurs during dynamic syncing of cem-xconnect configurations to the standby.

  Workaround: Apply reconfiguration CLIs through TFTP. If the reconfiguration CLIs are done in the router, the crash is observed.

- CSCui24744

  Symptom: An iosd crash is seen.

  Conditions: This symptom occurs on removing **bfd-template single-hop sw-no-echo-sha1** configuration.

  Workaround: There is no workaround.

- CSCui32105

  Symptom: In rare occasions the standby RP on a dual RP system may crash after performing a switchover.

  Conditions: This symptom occurs when an invalid message is sent from the RP to the RRP.

  Workaround: There is no workaround.

- 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.

- CSCui47602

  Symptom: Traces at IDMGR-3-INVALID_ID when queried for mplsTunnelTable MIB.

  Conditions: This symptom occurs when there is a GETONE SNMP query for non-existing mplsTunnelTable entries.

  Workaround: Avoid using GETONE SNMP query for non-existing objects. Use GETNEXT queries instead of GETONE whenever possible.

- CSCui49185

  Symptom: On a Cisco IOS ASR 1002x series router running Cisco IOS Release 15.4(01)S, a crash occurs.

  Conditions: This symptom occurs when MLDP over GRE is configured, with paths being added and removed. The counter of the number of paths in a CEF path list is not updated correctly. When they wrap at 256 this may cause a crash. The problem occurs when a path is removed without decrementing the counter properly. The problem is observed when a path is added/removed from a path list 256 times.

  Workaround: Do not modify paths using the method described.

- 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.

- CSCui53213

  Symptom: Traffic forwards through the VC even when the EVC is in a shut state.

  Conditions: This symptom occurs in scalable EoMPLS.

  Workaround: There is no workaround.

- CSCui56771

  Symptom: When **shutdown** and **no shutdown** are executed at an external interface on a router acting as a PfR border, the router may unexpectedly reload.

  Conditions: This symptom occurs on a Cisco router when heavy traffic is going through an external interface.

  Workaround: There is no workaround.

- CSCui62441

  Symptom: Complete traffic drop for few seconds is seen after few minutes of performing SSO switchover.

  Conditions: This symptom occurs only after a few minutes of performing an SSO switchover.

  Workaround: There is no workaround.

- 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: The symptom is observed on ES+ series linecards of Cisco 7600 Series Routers.

  Workaround: There is no workaround.

- CSCui67308

  Symptom: Cisco IOS Router constantly crashes after enabling TE tunnel over BDI interface.

  Conditions: This symptom is observed when TE tunnel is exits a BDI interface. This is not a supported design.

  Workaround: Use physical interface for TE tunnels.

- CSCui71298

  Symptom: A router crash is observed.

  Conditions: This symptom occurs when the configuration is replaced with CEM circuit.

  Workaround: There is no workaround.

- CSCui72518

  Symptom: A tunnel down (times out) occurs when the primary link is used again following FRR.

Conditions: This symptom occurs with FRR and reoptimizing the path back to the primary link with RSVP authentication enabled globally.

Workaround: Use interface CFG for RSVP authentication, as it has least impact on data traffic. The only fall out would be that the reopt may fail leaving FRR active LSP to timeout which will then impact traffic. The global CFG model can be used if you always use multi-hop backup tunnels.

- CSCui74609

  Symptom: After an 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 under the following conditions:

  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.

- 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.

- 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.

- CSCui95398

  Symptom: Config CLI to enable and disable the diag gives a false alarm detection and fails.

  Conditions: This symptom occurs when sprp_inband ping test fails.

  Workaround: There is no workaround.

- CSCui95880

  Symptom: HSRP for IPv6 flaps when there is a loop in the network, but IPv4 HSRP state remains stable for the same vlan.

  ```
  %HSRP-5-STATECHANGE: Vlan154 Grp 154 state Speak -> Standby %HSRP-5-STATECHANGE:
  Vlan154 Grp 154 state Standby -> Listen %HSRP-5-STATECHANGE: Vlan154 Grp 154 state
  Standby -> Listen %HSRP-5-STATECHANGE: Vlan154 Grp 154 state Speak -> Standby
  %HSRP-5-STATECHANGE: Vlan154 Grp 154 state Standby -> Active
  ```

  Conditions: This symptom is observed when a Layer 2 loop is in the network.

  Workaround: Create an IPv6 access-list, denying udp traffic sourced from device own Ipv6 link local address to any address & permit all other traffic. Apply that access-list to svi interface in inbound direction on the respective HSRP cores running IPv6 HSRP, then the HSRP group will not flap.

- 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. Re-configuring the VPLS circuit is also successful with a different local label assigned.

- CSCuj04178

  Symptom: A crash occurs at vpdn_apply_vpdn_template_pptp.

  Conditions: The conditions for this symptom are unknown.

  Workaround: There is no workaround.

- 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.

- CSCuj16367

  Symptom: Traffic does not flow on a few multilinks.

  Conditions: This symptom occurs during a microcode reload (due to any exception) during a multilink flap in Prowler SPA in SIP-400. This sometimes results in the DNR getting stuck.

  Workaround: Reload the SPA.

- 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.

- 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 under the following conditions:

  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.

- CSCuj47238

  Symptom: There is a difference in the Y1731 probe within **show ip sla statistics**.

  Conditions: This symptom is seen in the Cisco 7600 series routers.

```
service instance 400 ethernet evc1000 description -- EVC Cliente BUSINESS---
encapsulation dot1q 400 second-dot1q 100 <==HERE rewrite ingress tag pop 2 symmetric
<==HERE xconnect 172.16.12.6 1000 encapsulation mpls cfm mep domain OPM mpid 2
mdr-rm01#sh ip sla statistics 1 IPSLAs Latest Operation Statistics
IPSLA operation id: 1 Delay Statistics for Y1731 Operation 1 Type of operation: Y1731
Delay Measurement Latest operation start time: 12:06:21.041 CET Wed Sep 11 2013 Latest
operation return code: OK Distribution Statistics:
Interval Start time: 12:06:21.041 CET Wed Sep 11 2013 Elapsed time: 50 seconds Number
of measurements initiated: 44 <== HERE Number of measurements completed: 32 <== HERE
Flag: OK
```

  Workaround: There is no 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.

- CSCuj55914

  Symptom: The MPLS label of the labeled route is missing. This causes a traffic loss as only one path (non-labeled path) takes on the full load of the shared traffic setup.

  Conditions: This symptom occurs when there are two routes to a network and one of them is a sham-link, and the routes are learned via OSPF and redistributed by BGP, and one of the routes is labeled and the other is not, and the unlabeled route gets installed after the labeled route (for example, flapping). And both of the routes have the same metrics (that is, show ip route vrf <> x.x.x.x and show ip cef vrf <> x.x.x.x will have both entries).

  Workaround: Flap the unlabeled route and then the labeled route.

- 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.

- 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.

- CSCuj64806

  Symptom: VRRPv2 priority may be incorrectly calculated when tracking tunnel interfaces. After reloading the router, the track decrement value is decremented twice. As a result, VRRPv2 with tracking does not work as expected.

  Conditions: This symptom is observed when you use tracking tunnel for VRRP priority.

  Workaround: Use VRRPv3.

- 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.

- CSCuj68109

  Symptom: The Cisco 7600-SIP-400 router crashes.

Conditions: This symptom occurs when there is an Egress ESF Engine: ME Breakpoint error.

Workaround: There is no workaround.

- 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.

- 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.

- CSCuj87734

  Symptom: NVRAM startup configuration fails to load.

  Conditions: This symptom occurs on enabling the service compress configuration.

  Workaround: Disable the compress configuration CLI and save the configuration and reload the chassis. The chassis comes up with the NVRAM configuration.

- 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**

- CSCuj89036

  Symptom: IOSd crashes following an OIR of an eToken..

  Conditions: This symptom occurs during OIR activity on either USB port of a single eToken.

  Workaround: Do not OIR an eToken.

  More Info: When an eToken is inserted, files on the eToken need to be recursively scanned to build up the master file directory structure. This recursive scanning and building the database can take a very long time depending on the eToken contents. When dual IOSd redundancy mode is enabled, this process appears to take almost twice as long and can easily go over 10 seconds to trip off the IOSd watchdog timeout. Fix is to allow other processes to take over CPU so watchdog timeout will not happen.

- 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 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.

- CSCuj96186

  Symptom: When auto-tunnel and RSVP graceful restart are configured, the standby crashes after an SSO (NSR is not configured).

  Conditions: This symptom occurs under the following conditions:

  - Configure auto-tunnel
  - Configure RSVP graceful restart without NSR
  - Perform an SSO

  Workaround: Disable RSVP graceful restart or remove the auto-tunnel configuration.

- 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

- CSCul04006

  Symptom: The c7600rsp72043 router crashes while booting from the bootdisk with the following error message:

  ```
  Unable to open file to add LC tar
  bootdisk:c7600rsp72043-advipservicesk9-mz.152-4.S3a.bin
  ```

  Conditions: This symptom occurs while booting from the "bootdisk" on a c7600rsp72043 router.

  Workaround:

  1. After the new image file or the image file which is to be upgraded is copied to "sup-bootdisk", run the verify command to check that the new image file is copied properly. "verify /md5 sup-bootdisk:/<new-image-file> <expected-checksum>". The expected checksum can be found from the CCO site. If "verify" succeeds, then the new image can be booted.

2. Format “sup-bootdisk” and copy the new image to “sup-bootdisk” and run the “verify” command as mentioned above. If "verify" succeeds, then the boot can be tried.

- CSCul04692

  Symptom: A T1 controller flaps in CHT1/ET1 SPA.

  Conditions: This symptom is seen in T1 mode with “cablelength short 100ft” or “cablelength long 0db” when connected with a PURA box.

  Workaround: Configure “cablelength long -7.5db”.

- CSCul11738

  Symptom: Scaling to maximum number of TE tunnels fails.

  Conditions: This symptom occurs when there are sufficient tail-end tunnels on the node.

  Workaround: There is no workaround.

- CSCul11961

  Symptom: While performing an ISSU super-pkg downgrade with broadband IP-based session features from Cisco IOS XE Release 3.12.0 to Cisco IOS XE Release 3.11.0, standby FP gets stuck in an "init" state after run version. There are Standby FP pending issues.

  Conditions: This symptom occurs while performing an ISSU super-pkg downgrade with broadband IP-based session features from Cisco IOS XE Release 3.12.0 to Cisco IOS XE Release 3.11.0.

  Workaround: There is no workaround.

  More Info: The issue will not occurs in the following cases:

  1. ISSU sub-pkg upgrade or downgrade between XE311 and XE312.
  2. ISSU sup-pkg upgrade from XE311 to XE312.
  3. PPP-session features in ISSU super-pkg upgrade or downgrade between XE311 and XE312.

  The upgrade from 3.11.0(without the fix for CSCul11961) to 3.12(with the fix of CSCul11961) works fine.

  The downgrade from 3.12(with the fix of CSCul11961) to 3.11.0(without the fix for CSCul11961) fails with IP-based sessions. With this downgrade bug for 3.11.0, the fix will go out in 3.11.1 and 3.12.0.

- 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.

- CSCul12583

  Symptom: L4R is not removed after an account logon when DRL is present.

  Conditions: This symptom occurs if per user merge is present.

  Workaround: There is no workaround.

- CSCul24025

  Symptom: A Cisco ASR 1000 Series router crashes when the **ip sla udp-jitter** command is unconfigured.

Conditions: This symptom occurs when 1000+ IP SLA udp-jitter is configured and then all unconfigured immediately.

Workaround: There is no workaround.

- 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.

- CSCul31953

  Symptom: The wrong value is fetched for plaintext mtu of IPSec SA.

  Conditions: This symptom occurs while configuring Cisco Group Encrypted Transport VPN(GETVPN) within LISP network.

  Workaround: There is no known workaround.

- CSCul38081

  Symptom: In a scaled environment, when a preferred path configuration is removed and is followed by a RP switchover the pseudowire interfaces goes down. The psudowire interface comes up if we add the preferred path or just remove and add the neighbor statement.

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

  Workaround: There is no workaround.

- CSCul40176

  Symptom: PBR next-hop verify availability for global does not work after a reload.

  Conditions: This symptom occurs in **show run** after a reload.

  Workaround: There is no workaround.

- 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.

- CSCul42480

  Symptom: A router crashes upon booting due to lack of memory for the image.

  Conditions: There are no specific conditions for this symptom.

  Workaround: There is no workaround.

- 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.

- CSCul49852

  Symptom: A router might see PPPoE-sessions in the WAITING_FOR_STATS (or WT_ST) status.

  Conditions: This symptom was observed by specific users or because of using a specific profile or service like ShellMaps and Radius. The system is configured as BRAS aggregating PPPoEoA or -oE-sessions.

  Workaround: There is no workaround.

- CSCul50910

  Symptom: After a random reload of chassis or SPA Gig on SPA-5X1GE-V2 loses L3 connectivity and ARP protocol failing.

  Conditions: This symptom is observed in the Cisco 7600 router with SPA-5X1GE-V2.

  Workaround: Reload SIP with SPA loaded in it.

- CSCul52239

  Symptom: Multicast traffic might get affected after an interface delete and reconfiguration. This is more likely to happen in dot1q sub-interfaces in ES+ and specifically only if the delete and reconfiguration of the interface is done within 30 seconds.

  Conditions: This symptom occurs in Cisco IOS Release 12.2SREx and Cisco IOS 15S based releases.

  Workaround: Perform interface delete and reconfiguration with a time gap of one minute.

  More Info: How to check whether the issue is hit:

  Note down the interface's internal vlan:

  ```
  PE2#sh vlan int usage | i GigabitEthernet2/24.904 2000 GigabitEthernet2/24.904
  Get to SP console and do "sh fid start <internal vlan> end <internal vlan>
  PE2-sp#sh fid start 2000 end 2000 FID Id Protocol Bkt Enabled FE CAM Enabled Vlan
  Don't Learn Age group ------ -------------------- -------------- ---- -----------
  --------- 2000 no no 2000 yes 0x00
  ```

  The issue is hit if "FE CAM Enabled" bit is set to "no".

- CSCul56207

  Symptom: A standby RP crashes.

  Conditions: This symptom is seen on a Cisco ASR 1000 router used for PPPoEoA-aggregation when configuring a range/pvc. It was seen together with the following error message:

```
asr(config-if-atm-range)pvc-in-range 10/45 %ERROR: Standby doesn't support this
command ^ % Invalid input detected at '^' marker.
```

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.

- CSCul72121

  Symptom: Continuous trace backs on the PTF console is observed and PTF crashes during a soak.

  Conditions: This symptom occurs under the following conditions:

  1. Create an MDS profile as attached.
  2. Leave the setup for soak for 12 hours.

  Workaround: Reload ACT and SBY PTF.

- 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.

- 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 signaling 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.

- CSCul99015

  Symptom: In VPLS using BGP signaling with Inter AS, when a PE on another AS is reachable through multiple ASBRs, the PW destination and the next hop PE address of some or all of the PWs in the standby RP remains as the non-preferred ASBR address instead of the preferred ASBR address.

  Conditions: This symptom occurs under the following conditions: 1. BGP L2VPN NLRIs received first from an ASBR becomes a less preferred ASBR on receiving NLRIs for the same VE-IDs from a more preferred ASBR. 2. NLRI received from the more preferred ASBR has the same values (VEID, VBO, VBS, Label Base, MTU and CW) as the ones received previously from the other ASBR.

  Workaround: Bring up the BGP session with the more preferred ASBR first. This would cause no updates to existing NLRIs even if received from other less preferred ASBRs.

- 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.

- CSCum04512

  Symptom: When an RP switchover is done (which is head end for 500 TE tunnel and tail end for 500 TE tunnels), the RSVP label is assigned to the TE tunnel change and this in turn causes a traffic loss of 45 seconds on the pseudowire which is directed through these tunnels.

  Conditions: This symptom occurs under the following conditions:

  - TE RID under the IGP is configured as a loopback other than the first one.
  - SSO is performed.

  Workaround: Configure the TE router ID under the IGP to be the first loopback interface.

- CSCum11118

  Symptom: A Cisco ISR router crashes due to stack overflow in the “ADJ background” process. The following syslog may be seen just before the crash:

```
000105: Dec 9 04:08:44.447 UTC: SYS-6-STACKLOW Stack for process ADJ background
running low, 20/6000
```

Conditions: The conditions to this symptom are unknown.

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 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 :
```

- CSCum20242

  Symptom: The RSP720 image bootup fails with the following messages:

```
rommon 2 > boot disk0:rsp72043-adventerprisek9-mz Initializing ATA monitor library...
Self extracting the image... [OK] Error : memory requirements exceed available memory
Memory required : 0x40286C44 *** System received a Software forced crash *** signal=
0x17, code= 0x4, context= 0x0
```

  Conditions: This symptom could occur when the image size is very big (approximately greater than 220MB). This is not reported in any production images so far because their size is not big enough to hit this issue.

  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 7600 Series Routers after SSO is performed on PE with L2VPN in PFC vlan mode is configured

  Workaround:

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

- CSCum34830

  Symptom: A router crash is observed.

  Conditions: This symptom occurs while performing VRRP and VRRS-related configuration changes.

  Workaround: Unconfigure the **ip pim redundancy <>** command before deleting the subinterface or disabling PIM on an interface.

- CSCum42586

  Symptom: SLM does not work over the port-channel evc xconnect up mep.

Conditions: This symptom occurs when port-channel member links are on the same NP.

Workaround: There is no workaround.

- CSCum46850

  Symptom: Using LISP set tags on routes imported to the RIB when exporting LISP routes from the RIB to BGP fails.

  Conditions: This symptom occurs when redistribute list route-map is used under bgp with a route-map that contains match tag.

  Workaround: There is no workaround.

- CSCum62783

  Symptom: The following alignment errors are seen after a PPPoE session establishment for the first time after a reboot:

  ```
  *Jan 14 07:24:40.591: %ALIGN-3-CORRECT: Alignment correction made at 0x32B2DFF4z
  reading 0xE7790ED *Jan 14 07:24:40.591: %ALIGN-3-TRACE: -Traceback= 0x32B2DFF4z
  0x32B1E274z 0x32B1EECCz 0x32B1EF90z 0x332E550Cz 0x332E54F0z 0xFFFF1A00z 0xFFFF1A00z
  ```

  Conditions: This symptom occurs when **pppoe-client ppp-max-payload** is configured under the Ethernet interface.

  Workaround: There is no workaround.

- 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.

- CSCum67166

  Symptom: The router hangs after loading an image.

  Conditions: This symptom occurs with the latest whales-universal-mz mcp_dev image.

  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.

- CSCun38333

  Symptom: Locator ID Separation Protocol (LISP) local EID database locator configured through the "**database-mapping** <*eid-prefix*> **ipv6-interface** <*interface*> **priority** <*priority*> **weight** <*weight*>" command uses deprecated IPv6 address on specified interface.

  Conditions: Multiple IPv6 addresses available on an interface with the lexicographically first address being deprecated.

  Workaround: There is no workaround.

- CSCun57668

Symptom: LISP local EID database locator configured through the **database-mapping <***eid-prefix***> ipv6-interface <***interface***> priority <***priority***> weight <***weight***>** command can be a deprecated IPv6 address on a specified interface.

Conditions: This symptom is observed in multiple IPv6 addresses available on an interface with the lexicographically first address being deprecated.

Workaround: There is no workaround.

Open and Resolved Bugs - Cisco ASR 901 Series Routers in 15.4(2)S

For detailed information on Open and Resolved bugs on Cisco ASR 901 Series Routers in 15.4(2)S, see the following document:

https://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Release/Notes/b-901-rn-15-4-2.html

Open and Resolved Bugs - Cisco ASR 901 S Series Routers in 15.4(2)S

For detailed information on Open and Resolved bugs on Cisco ASR 901 S Series Routers in 15.4(2)S, see the following document:

https://www.cisco.com/c/en/us/td/docs/wireless/asr_901s/scg/b_scg_for_asr901s.html

Open and Resolved Bugs - Cisco ME 3600x and ME 3800x Series Routers in 15.4(2)S

For detailed information on Open and Resolved bugs on Cisco ME 3600x and Cisco ME 3800x Series Routers in Cisco IOS Release 15.4(2)S, see the following document:

http://www.cisco.com/c/en/us/support/switches/me-3600x-series-ethernet-access-switches/products-release-notes-list.html