Caveats for Cisco IOS Release 15.2(1)S

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

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

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

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

This section consists of the following subsections:

- Resolved Caveats—Cisco IOS Release 15.2(1)S2, page 373
- Resolved Caveats—Cisco IOS Release 15.2(1)S1, page 385
- Open Caveats—Cisco IOS Release 15.2(1)S, page 403
- Resolved Caveats—Cisco IOS Release 15.2(1)S, page 414

Resolved Caveats—Cisco IOS Release 15.2(1)S2

Cisco IOS Release 15.2(1)S2 is a rebuild release for Cisco IOS Release 15.2(1)S. The caveats in this section are resolved in Cisco IOS Release 15.2(1)S2 but may be open in previous Cisco IOS releases.

- CSCti00319

  Symptom 1: The warning message “Fatal error FIFO” occurs repeatedly upon PPPoEoA Session teardown.

  Symptom 2: On the LC console, the message “Command Indication Q wrapped” keeps appearing.

  Conditions: This symptom is observed on a Cisco ASR1001 router and kingpin router chassis under the following conditions:

  1. High scale session counts.
  2. Range configuration with more than 100 virtual channels (VC).
  3. Back to back creation and deletion of multiple VCs with no time gap.

  Workaround: There is no workaround.

- CSCtj95685

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

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

  Workaround: There is no workaround.

- CSCtq24557

  Symptoms: Router crash after deleting multiple VRFs. This happens very rarely.

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

  Workaround: There is no workaround.

- CSCtq95384

  Symptoms: Even after the removal of NSR configurations, BGP still holds memory.

  Conditions: The symptom is observed after the removal of NSR configurations.

  Workaround: There is no workaround.

- CSCtr47317

  Symptoms: After a switchover, a Cisco Catalyst 6500 series switch may be replicating some spanned traffic indefinitely and flooding the network with the span copies.

  Conditions: The issue is seen after the following sequence:

  – An internal service module session for a FWSM or other service modules exists:

```
UUT#show monitor session all
Session 1
Type   : Service Module Session
```

  – If you attempt to configure a span session with the session number already in use:

```
UUT(config)#monitor session 1 source interface Gi2/7 , Gi2/40
% Session 1 used by service module
```

  – The command seems to be rejected, but it is synchronized to the standby supervisor.

  – A switchover happens.

  Workaround: There is no workaround.

- CSCtr87070

  Symptoms: Enable login failed with error “% Error in authentication”.

  Conditions: The symptom is observed with TACACS single-connection.

  Workaround: Remove TACACS single-connection.

- CSCts40043

  Symptoms: A Cisco router may crash due to a segmentation fault.

  Conditions: The symptom is observed when a fail-close ACL is applied to the Gdoi crypto map in GETVPN implementation.

  Workaround: There is no workaround.

- CSCts59564

  Symptoms: PIM neighbor over MDT tunnel goes down.

  Conditions: The symptom is observed with **hw-module reset** of access and core card, followed by an SSO.

  Workaround: There is no workaround.

- CSCts65564

  Symptoms: In a large scale DMVPN environment, a DMVPN hub router may crash in the IOS process under high scale conditions.

  Conditions: This only occurs if CRL caching is disabled (with the command **crl cache none** under the pki trustpoint configuration).

Workaround: Enable CRL caching (this is the configured default).

- CSCts72911

  Symptoms: In case of a GR/NSF peering, after an SSO switchover, the restarting router (PE, in this case) does not advertise RT constrain filters to the non-restarting peer (RR, in this case).

  Conditions: The symptom is observed after an SSO switchover in GR/NSF peering. Due to the RT constrain filters not sent by the restarting router after the SSO, the non-restarting router does not send back the corresponding VPN prefixes towards the restarted router.

  Workaround: There is no workaround.

- CSCts88817

  Symptoms: ASA-SM(s) and SCV-NAM3 in a Cisco Catalyst 6000 series switch may be reloaded by supervisor associated with the following syslogs reported by the switch:

```
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 31
seconds [4/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 31
seconds [9/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 61
seconds [4/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 61
seconds [9/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 91
seconds [4/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 91
seconds [9/0]
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled 'off (Module not
responding to Keep Alive polling)'
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Module not
responding to Keep Alive polling)
%OIR-SP-3-PWRCYCLE: Card in module 9, is being power-cycled 'off (Module not
responding to Keep Alive polling)'
 %C6KPWR-SP-4-DISABLED: power to module in slot 9 set off (Module not
responding to Keep Alive polling)
```

  Conditions: The lockup may occur if there are non-fabric cards in the chassis with the ASA or NAM3 card. Non-fabric cards have a model number of 61xx, 62xx, 63xx, and 64xx.

  Workaround: There is no workaround.

- CSCtt17762

  Symptoms: Mtrace does not show the IP address of RPF interface of a multicast hop.

  Conditions: The symptom is observed on an IP PIM multicast network.

  Workaround: There is no workaround.

- CSCtt26074

  Symptoms: Memory leak with IP SLAs XOS Even process.

  Conditions: The symptom is observed with IP SLA configured.

  Workaround: There is no workaround.

- CSCtt35379

  Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

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

- CSCtt39944

  Symptoms: The **show mls cef adjacency usage** is not showing the adjacency count correctly.

  Conditions: The symptom is observed in highly scaled networks. The platform code is not counting the last non-stats region allocation for adjacency usage.

  Workaround: There is no workaround.

- CSCtt46638

  Symptoms: A Cisco 7604 running Cisco IOS Release 12.2(33)SRE4/SRE5 crashes when changing the tunnel source and destination of an IPsec sVTI.

  Conditions: The symptom is observed once the IPsec session is up and traffic is flowing through. If the tunnel source or destination is changed, the router crashes. This does not occur with a plain GRE tunnel.

  Workaround: There is no workaround.

- CSCtu00699

  Symptoms: On a DMVPN hub router, the IOS processor memory pool can get fragmented due to memory allocated for “Crypto NAS Port ID”.

  Conditions: This happens when there is network instability potentially causing tunnels to flap frequently.

  Workaround: There is no workaround.

- CSCtu08608

  Symptoms: The standby RP crashes due to Voip HA Session App.

  Conditions: The Cisco ASR 1000 platform with redundant RPs and Cisco Unified Border Element Enterprise. The signature in the crashinfo is as follows:

  ```
  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Voip HA Session App
  ```

  Workaround: There is no workaround.

- CSCtu26431

  Symptoms: Memory leaks pointing to “OER SAA MC PROB”.

  Conditions: The symptom is observed when running probes are deleted. This is a rare event.

  Workaround: There is no workaround.

- CSCtu32301

  Symptoms: Memory leak may be seen.

  Conditions: This is seen when running large **show** commands like **show tech-support** on the linecard via the RP console.

  Workaround: Do not run the show commands frequently.

- CSCtu35116

  Symptoms: VPDN session keeps on trying to come up with MPLS MTU higher than 1500.

Conditions: The symptom is observed when you upgrade a Cisco 7200VXR from the c7200-a3jk91s-mz.122-31.SB18 to the c7200-adventerprisek9-mz.122-33.SRE4 image.

Workaround: There is no workaround.

- CSCtu38244

  Symptoms: After bootup, the GM cannot register and is stuck in "registering" state. Issuing the **clear crypto gdoi** command is required for a successful registration to the keyserver.

  Conditions: The symptom is observed upon router bootup.

  Workaround: Either do a **clear crypto gdoi** after a reload, or configure a second keyserver entry. This does not have to be an existing keyserver, it can be just a dummy address.

- CSCtu60863

  Symptoms: IGMP reports do not get installed in the IGMP group list.

  Conditions: The symptom is observed when the port-security feature is enabled on the switchport which is part of the VLAN on which the IGMP reports are received.

  Workaround: Remove "switchport port-security" from ports associated with the VLAN on which the IGMP reports are received.

- CSCtu65655

  Symptoms: RP1 crash due to corrupted memory.

  Conditions: The symptom is observed with the following conditions:

  - Ixia -- CES (IPsec static crypto map) -- UUT (IPSec DVTI server).
  - UUT - 4RU(RP1/ESP10).
  - Scale 1000 IKE * 1 VRF * 4 IPsec, total 4K IPsec sessions.
  - CAC (30) enabled.
  - DPD (60/15/on-demand) enabled.
  - Reload CES (Cisco 7200 platform) every 10-15 minutes.
  - 60M bidirectional traffic.

  Workaround: There is no workaround.

- CSCtw45592

  Symptoms: The **ntp server** *DNS-name* command is not synced to the standby. When the **no ntp server** *hostname* command is issued later on the active, the standby reloads because the config was not added.

  Conditions: When the device is reloaded or when the DNS name is not resolved, the config is not added. After the standby SYNC failure, then issuing the **no ntp server** *hostname*.

  Workaround: Use IP/IPv6 addresses instead of the hostname for NTP configurations. The IP/IPv6 address can be found by pinging the hostname.

- CSCtw56439

  Symptoms: The **ip mtu** command that is configured on an IPsec tunnel disappears after a router reload.

  Conditions: The symptom is observed with IPsec and the **ip mtu** over a tunnel interface.

  Workaround: There is no workaround.

- CSCtw61872

  Symptoms: The router will crash when executing a complex sort on the flexible netflow cache from multiple CLI sessions.

  Conditions: The symptom is observed when executing a complex sort with top- talkers on a show command from multiple CLI sessions (note that normal show commands without top-talkers are fine):

  ```
  sh flow monitor QoS_Monitor cache sort highest counter packets top 1000
  sh flow monitor QoS_Monitor cache sort highest counter packets top 10000
  ```

  Workaround: Do not execute complex sorts with top-talkers on the show output from multiple CLI sessions.

- CSCtw62310

  Symptoms: The **cells** keyword is added to “random-detect” whenever a policy-map is removed from an interface/map-class via “no service- policy”.

  Conditions: The symptom is observed when removing the policy-map from map-class.

  Workaround: There is no workaround.

  Further Problem Description: The CLI is technically valid if it has been manually configured as “cells” prior to the removal. The issue is that the template policy is being changed automatically to “cells” whenever the removal happens, regardless of what the original configuration was, and that is not the expected behavior.

- CSCtw71564

  Symptoms: Not all data packets are accounted for in the “show stats” output of the video operation.

  Conditions: The symptom is observed with heavy load on the responder caused either by many video sessions or other processes.

  Workaround: Reduce processor load on device running the responder.

- CSCtw78451

  Symptoms: A Cisco ASR 1000 series router may reload when multiple users are logged in running show commands.

  Conditions: This symptom is only seen when the Cisco ASR router is used as a DMVPN headend and there are hundreds of tunnels flapping.

  Workaround: There is no workaround. However, this appears to be a timing issue when there is instability in a large-scale environment.

- CSCtw86712

  Symptoms: RP crashes.

  Conditions: The symptom is observed when you apply certain tunnel configurations.

  Workaround: There is no workaround.

- CSCtw88094

  Symptoms: The standby management processor reloads during configuration sync when there is a mismatch in the IP SLA configuration.

  Conditions: This symptom occurs shortly after the “ip sla schedule X start specific_start_time” command is issued multiple times on the same probe instance. Hence, when the configuration is synced to the standby management processor, a PRC error occurs. The PRC error causes a reload of the standby management processor.

  Workaround: Unschedule the probe before rescheduling for a specific start time.

- CSCtw88599

  Symptoms: If “port acl” is configured, diagnostics for the port fail during bootup. If the port ACL is on a supervisor port then the router goes for a reload.

  Conditions: The symptom is observed when you configure “port acl” on a switch port and reload the router.

  Workaround: Disable diagnostics for the module.

- CSCtw94598

  Symptoms: Web authentication does not work after an upgrade. NAS-Port-Type = Async.

  Conditions: The symptom is observed when you upgrade to Cisco IOS Release 12.2 (58)SE2 or later or to the Cisco IOS 15.0(1)SE train.

  Workaround: Change NAS-Port-Type on AAA Server to match the new value.

- CSCtw98456

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

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

  For example, the IVRF routing table should show:

  ```
  S        10.0.0.0 [1/0] via 192.168.0.1, GigabitEthernet1/0/1
  ```
  but instead it shows:

  ```
  S        10.0.0.0 [1/0] via 192.168.0.1
  ```
  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

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

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

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

  ```
  ip route vrf IVRF 10.0.0.0 255.0.0.0 GigabitEthernet1/0/1 192.168.0.1
  ```
  where GigabitEthernet1/0/1 is the interface in the FVRF with the crypto map, and 192.168.0.1 is the next-hop in the FVRF through which the VPN peer is reachable.

- CSCtw99989

  Symptoms: During normal operation a Cisco ASR 1000 Series Aggregation Services router may show the following traceback:

  ```
  %FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi
  ```
  Conditions: The symptom is observed during PPP renegotiation.

  Workaround: There is no workaround.

- CSCtx02522

  Symptoms: The router displays intermittent traceback errors.

  Conditions: Occurs when you configure REP.

  Workaround: There is no workaround.

- CSCtx29543

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

  Conditions: This symptom occurs under the following conditions:

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

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

  Workaround: There are two possible workarounds:

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

- CSCtx31175

  Symptoms: Framed-IP-Address added twice in PPP service-stop accounting record.

  Conditions: The symptom is observed with the following conditions:

  1. User session exists on ASR1001.
  2. Stop one user's session by using **clear subscriber session username xxx** on ASR1001.
  3. ASR1001 sends double "Framed-IP-Address" in service-stop accounting for one user's session.

  Workaround: Do not use **clear subscriber session** command to clear the session, instead use **clear pppoe**.

- CSCtx32628

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

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

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

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

- CSCtx35692

  Symptoms: On the Cisco ASR 1000 platform, while acting in a redundancy pair, when the standby ASR becomes active the dial-peers on the standby never change their state back to active causing all calls to fail. Calls that were active during the failover scenario will stay active in the new switchover. Only new calls are affected.

Conditions: The symptom is observed on an ASR 1000 series router CUBE with a box-to-box redundancy configured that is using OOD option pings in the dial- peers. Global configuration of option pings under voice service VoIP is only for IN-Dialog option pings.

Workaround: Disable option keepalives from the dial-peers.

- CSCtx39936

  Symptoms: A Cisco 7600 router configured for MPLS TE with tunnel load-sharing may punt traffic to MSFC when multiple TE paths to a given destination exist.

  Conditions: The symptom is observed with a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRE4, configured with multiple MPLS TE tunnels with load-sharing.

  Workaround 1: In some cases, clearing the router may trigger proper reprogramming of the prefix in the hardware.

  Workaround 2: Remove load-sharing from the TE tunnels.

- CSCtx48010

  Symptoms: PIM neighbors on MDT tunnel continuously flap on a Cisco 7600 series router. Decapsulation path shows wrong rewrite index for flapping peers, instead of expected 7FFA recirculation index.

  Conditions: The symptom is observed with Cisco IOS Release 15.1(3)S1. ES20 card as core-facing.

  Workaround: Identifying the adjacency of the flapping peer and changing the rewrite index to 7FFA manually stops the flap:

  ```
  test mls cef adj 180262 4055 9238 7ffa 2608 20 multicast 001e.f741.e28d 0.0.0 0 0x5fa
  ```

- CSCtx49073

  Symptoms: Free space check fails and IOS core dump never completes.

  Conditions: The symptom is observed when there is not enough storage media space for IOS core dump.

  Workaround: Make sure there is enough storage space for IOS core dump.

- CSCtx51935

  Symptoms: Router crashes after configuring “mpls traffic-eng tunnels”.

  Conditions: The symptom is observed with the following steps:

  ```
  interface gi1/2
  mpls traffic-eng tunnels
  no shut

  router OSPF 1
  mpls traffic-eng area 100
  mpls traffic-eng router-id lo0
  end
  ```

  Workaround: There is no workaround.

- CSCtx55357

  Symptoms: Auto RP messages are permitted through “ip multicast boundary”.

  Conditions: The symptom is observed when the ACL associated with the multicast boundary matches 224.0.1.39 and 224.0.1.40. It is seen on the Cisco ASR 1000 platform.

  Workaround: Use “no ip pim autorp” which will disable Auto RP completely from this device.

- CSCtx61815

  Symptoms: IPsec sessions are not coming up.

Conditions: The symptom is observed when 1000 sessions are configured. Only 50 IPsec sessions are coming up.

Workaround: There is no workaround.

- CSCtx67474

  Symptoms: Update message is sent with an empty NLRI when the message consists of 2byte aspath in ASPATH attribute and 4byte value aggregate attribute.

  Conditions: This can happen when there is a mix of 2byte and 4byte attributes in the update message and the message is sent from a 2byte peer and there is a 4byte aggregator attribute.

  Workaround: Move all the 2byte AS peers to a separate update-group using a non-impacting outbound policy like “advertisement-interval”.

- CSCtx71618

  Symptoms: Router crash at process L2TP mgmt daemon.

  Conditions: The symptom is observed with a Cisco ASR 1006 (RP2) running Cisco IOS Release 15.1(2)S.

  Workaround: There is no workaround.

- CSCtx73452

  Symptoms: The following symptoms are observed:

  1. You send an ICMPv4 packet with IP option. It will be forwarded by ASR1001. IP options field includes “loose source routing” option.
  2. ASR 1001 receives the packet. ASR 1001 has “no ip source-route” setting in its configuration.
  3. ASR 1001 incorrectly overwrites the destination IP address of packet, which has source-route option set, and forwards it instead of dropping it.

  Conditions: The symptom is observed with the Cisco ASR 1001 (2.5G ESP).

  Workaround: There is no workaround.

- CSCtx73612

  Symptoms: A Cisco ASR 1000 may reload while reading IPsec MIBs via SNMP and write a crashfile.

  Conditions: The symptom is observed on a Cisco ASR 1000 that is running Cisco IOS Release 15.1(1)S1.

  Workaround: Do not poll or trap IPsec information via SNMP.

- CSCtx74342

  Symptoms: After interface goes down or is OIRed, in a routing table you can temporarily see IPv6 prefixes associated with the down interface itself (connected routes) as OSPFv3 with the next hop interface set to the interface that is down.

  Conditions: The symptom is observed with OSPFv3. The situation remains until the next SPF is run (5 sec default).

  Workaround: Configuring SPF throttle timer can change the interval.

  Further Problem Description: Here is an example of output after Ethernet0/0 goes down:

```
Routershow ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
```

```
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       l - LISP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   2001::/64 [110/10]
     via Ethernet0/0, directly connected
```

- CSCtx89260

  Symptoms: Re-adding the deleted port channel interface is not initializing the snmp-index.

  Conditions: The symptom is observed when re-adding the deleted port channel interface.

  Workaround: Reloading the standby and then doing an RP switchover or doing a double RP switchover corrects the configuration.

- CSCtx93598

  Symptoms: An “ikev1 dpd” configuration erroneously affects IKEv2 flows.

  Conditions: The symptom is observed if we configured the IKEv1 DPD function with “crypto isakmp keepalive” while IKEv2 is enabled as well. The IKEv2 DPD function will be affected.

  Workaround: There is no workaround.

- CSCtx99544

  Symptoms: Exception occurs when using **no aaa accounting system default vrf** *VRF3* **start-stop group** *RADIUS-SG-VRF3*:

```
router(config)# no ip vrf VRF3
router(config)# no aaa accounting system default vrf VRF3 start-stop group
RADIUS-SG-VRF3

%Software-forced reload
```

  Conditions: The symptom is observed with the following conditions:

  - Hardware: Cisco ASR 1001.
  - Software: asr1001-universalk9.03.04.02.S.151-3.S2.

  Workaround: There is no workaround.

- CSCty02403

  Symptoms: EIGRP topo entry with bogus nexthop is created when more than one attribute is present in the route received from neighbors. It also tries to install one default route with bogus nexthop. So if you have a default route received from some neighbors, then that default route will also be flapped.

  Conditions: It can only occur when you have more then one attribute set in any route received from a neighbor.

  Workaround: Do not set more then one attribute in the route.

- CSCty05150

  Symptoms: Default route is removed from stub area after SSO.

  Conditions: The symptom is observed when a PE router is configured as ABR for a stub area and generating a default route. After switchover the default route is withdrawn.

  Workaround 1: Move the default route generation to CE router.

  Workaround 2: Remove and reconfigure “area x stub no summary” on PE router.

- CSCty06191

  Symptoms: When an IPHC configuration is applied on a multilink bundle interface and the interface is flapped, the IPHC configuration does not apply successfully on a linecard.

Conditions: The symptom is observed with a multilink interface flap.

Workaround: Unconfigure and then reconfigure the IPHC configuration on the multilink interface.

- CSCty06990

  Symptoms: Intercepted packets are not forwarded to MD.

  Conditions: The symptom occurs randomly after applying an LI tap on a Cisco 7600 with a SIP400 as the dedicated LI service card.

  Workaround: Remove and reapply TAP.

- CSCty13647

  Symptoms: Symptoms vary from one image to another. The following symptoms have been mostly observed:

  1. Spurious memory access tracebacks from SPAN code even when SPAN is not configured.
  2. RP crash when unconfiguring a SPAN session with a particular session number.

  Conditions: Always seen on a particular SPAN session number.

  Workaround: Use a different a SPAN session number for SPAN configurations to avoid the router crash. (There is no workaround to avoid spurious memory access messages.)

- CSCty37020

  Symptoms: Learned inside BGP prefixes are not getting added into MC database.

  Conditions: The symptom is observed with learned inside BGP prefixes.

  Workaround: There is no workaround.

- CSCty37445

  Symptoms: A DMVPN hub router with a spoke which is an EIGRP neighbor. The spoke receives a subnet from hub and then advertises it back to the hub, bypassing split horizon.

  Conditions: The symptom is observed when on the spoke you have a **distribute list route-map** command setting tags.

  Workaround: Once you remove that command EIGRP works normally.

- CSCty43582

  Symptoms: The **port-channel load-balance-hash-algorithm** CLI is not saved properly in the running-configuration.

  Conditions: The symptom is observed when the hash algorithm chosen is one of src-ip, dst-ip, or src-dst-ip.

  Workaround: There is no workaround.

- CSCty58300

  Cisco IOS Software contains a vulnerability in the Border Gateway Protocol (BGP) routing protocol feature.

  The vulnerability can be triggered when the router receives a malformed attribute from a peer on an existing BGP session.

  Successful exploitation of this vulnerability can cause all BGP sessions to reset. Repeated exploitation may result in an inability to route packets to BGP neighbors during reconvergence times.

Cisco has released free software updates that address this vulnerability. There are no workarounds for this vulnerability. This advisory is available at the following link:

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

- CSCty58656

  Symptoms: A Cisco 7600 series router with ES+ module may crash.

  Conditions: The symptom is observed with the QoS policy map that has a name hash that is same as an existing policy used by the ES+ module and configuring a child policy or adding a child policy that is already in use.

  Workaround: Do not call a child policy map.

- CSCty60467

  Symptoms: SSM ID leak issues or SSM stats show unprovisioned segment counters. The leak can be observed with the command **show ssm stats**. Look for the following in the output:

```
Segment States Counters
  Type            Class           State           Count
  IP-SIP          SSS             Unprov          1050  <<< the count indicates the
IDs are getting leaked.
```

  Alarm: Counter reaches 1 Million: indicates you may be nearing ID exhaust state.

  Conditions: The symptom is observed with the following steps:

  1. Configure “ip dhcp ping packets 10” on an ISG.
  2. Initiate an L2-connected ISG DHCP session by triggering DHCP discover from the client.
  3. Start TCP traffic from the client immediately.
  4. The issue can be observed commonly on high CPS (greater than best practice).
  5. Observed in Cisco IOS XE Release 3.2 and XE 3.5.

  Workaround: Configuring “ip dhcp ping packets 0” will bring down the rate of SSM ID leak.

Resolved Caveats—Cisco IOS Release 15.2(1)S1

Cisco IOS Release 15.2(1)S1 is a rebuild release for Cisco IOS Release 15.2(1)S. The caveats in this section are resolved in Cisco IOS Release 15.2(1)S1 but may be open in previous Cisco IOS releases.

- CSCee38838

  Symptoms: A crashdump may occur during a two-call-per-second load test on a gateway, and the gateway may reload.

  Conditions: This symptom is observed on a Cisco 3745 that runs Cisco IOS Release 12.3(7)T and that functions as a gateway when you run a two-call-per-second load test that uses H.323, VXML, and HTTP. The crash occurs after approximately 200,000 calls.

  Workaround: There is no workaround.

- CSCsb53810

  Symptoms: A Cisco Catalyst 6500 series switch may not block traffic, which is supposed to be denied by an outbound ACL on a VLAN interface.

  Conditions: This issue is under investigation.

  Workaround: Reload the switch.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr : DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. If this not an option, there is no workaround.

- CSCtg57657

  Symptoms: A router is crashing at dhcp function.

  Conditions: This issue has been seen on a Cisco 7206VXR router that is running Cisco IOS Release 12.4(22)T3.

  Workaround: There is no workaround.

- CSCtg58029

  Symptoms: After switchover, aaa_acct_session_id iss not issued to new sessions.

  Conditions: This symptom occurs only after switchover.

  Workaround: There is no workaround.

- CSCtj33003

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

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

  This advisory is available at the following link:

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

- CSCtj64807

  Symptoms: Router crashes while issuing the **show vlans dot1q internal** command.

  Conditions: The symptom is observed with the following conditions:

  1. One QinQ subinterface configured with inner VLAN as “any”.
  2. More than 32 QinQ subinterfaces configured with same outer VLAN.
  3. All subinterfaces are removed except subinterface configured with “any” inner VLAN.

  Workaround 1: For any Cisco 10000 series router which has had its first crash on any subinterface if the outer VLAN has second-dot1q VLAN as only “any”, immediately delete the sub-interface and recreate it. Then add a dummy VLAN/sub-interface to this outer VLAN.

  Workaround 2: On any outer VLAN (in array state) if they have less than 5 inner VLANs, add a dummy VLAN/subinterface.

  Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with second-dot1q VLAN as only “any” and active sessions, add a dummy VLAN/sub-interface to this outer (tree state) VLAN.

- CSCtk00181

  Symptoms: Password aging with crypto configuration fails.

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

Workaround: There is no workaround.

- CSCtk62763

  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.

  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

  Workaround: There is no workaround.

- CSCtn02208

  Symptoms: Old PerUser ACL is not removed on applying new ACL.

  Conditions: This symptom occurs when applying a new PerUser ACL to an existing session. The old PerUser ACL that exists on the session is not removed.

  Workaround: There is no workaround.

- CSCtn40771

  Symptoms: The process ACL Header in the **show memory allocating- process totals** command output leaks memory with per-user ACLs and PPP session churn. This will also cause the SSS feature manager process in the **show process memory** command output to appear to have a leak.

  Conditions: This symptom occurs with IPv6 per-user ACLs and session churn.

  Workaround: There is no workaround.

- CSCto71671

  Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

  Workaround: There is no workaround.

- CSCtq59923

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

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

  Workaround: Configure “ip routing protocol purge interface”.

- CSCtr08680

  Symptoms: The following error messages are displayed on active and standby respectively:

  ```
  %ERROR: Standby doesn’t support this command BERT is running on this channel group,
  please abort bert first.
  ```

  Conditions: This symptom is observed when trying to create a channel after BERT has been started irrespective of whether BERT is running or completed.

  Workaround: There is no workaround.

- CSCtr45551

  Symptoms: T1/E1 controller does not get selected as network clock input source.

  Conditions: This symptom occurs when network-clock input source t1/e1 command is configured immediately after reload of the router or within 5 minutes from router bootup.

  Workaround: After the router reloads, wait for 5 to 6 minutes (until SETS gets initialized) and then configure T1/E1 as network clock input source.

- CSCtr47642

  Symptoms: On Cisco IOS Release 15.2(3)T that is running BGP configured as RR with multiple eGBP and iBGP non-clients and iBGP RR clients and enabling the BGP best-external feature using the **bgp additional-paths select best- external** command, a specific prefix may not have bestpath calculated for a long time.

  Conditions: The problem occurs on a certain condition of configuration of the below commands, and a few prefixes are withdrawn during the configuration time:

  1. Configure: **bgp additional-paths install** under vpnv4 AF
  2. Configure: **bgp additional-paths select best-external**

  Immediately disable backup path calculation/installation using the **no bgp additional-paths install** command.

  The problem does not appear if both of the above commands are configured with more than a 10-second delay as the commands will be executed independently in two bestpath runs instead of one.

  Workaround: Configure the **bgp additional-paths install** command and the **bgp additional-paths select best-external** command with a delay of 10 seconds.

- CSCtr88739

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

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

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

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

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

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

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

- CSCtr91106

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

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

Cisco has released free software updates that address these vulnerabilities.

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

This advisory is available at the following link:

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

- CSCts00341

  Symptoms: When executing a CLI that requires domain-name lookup such as **ntp server** *server.domain.com*, the command fails with the following message on the console:

```
ASR1k(config)#ntp server server.domain.com         <<<    DNS is not resolved
with dual RPs on ASR1k
Translating "server.domain.com "...domain server (10.1.1.1) [OK]

%ERROR: Standby doesn't support this command              ^
% Invalid input detected at '^' marker.

ASR1k(config)#do sh run | i ntp
ASR1k(config)#
```

  Conditions: This symptom occurs on a redundant RP chassis operating in SSO mode.

  Workaround: Instead of using *hostname* in the command, specify the IP address of the host.

- CSCts13255

  Symptoms: Standby SUP720 crash is observed on the Cisco 7600 router in c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

```
%CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive
heartbeats
```

  Conditions: This symptom is observed on the Cisco 7600 router with mistral based supervisors like SUP720. This issue is fairly uncommon, but affects all the versions after Cisco IOS Release 12.2(33)SRE, including Cisco IOS Releases 15.0S, 15.1S and 15.2S. This does not affect RSP 720.

  Workaround: There is no workaround.

- CSCts23882

  Symptoms: ISG calculates the radius response authenticator in CoA account- profile-status-query replies wrongly, resulting in an invalid response.

  Conditions: This symptom is observed when the CoA/WWW based session authentication is triggered via a CoA account logon using the “old” SSG command attributes.

  Workaround: Configure a fix “NAS-IP-Address” value with the **radius- server attribute 4** *x.x.x.x* command.

- CSCts38429

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

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

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

- CSCts67465

  Symptoms: If you configure a frequency greater than the enhanced history interval or if the enhanced history interval is not a multiple of the frequency, the standby will reset.

  Conditions: The symptom is observed always, if the standby is configured as an SSO.

  Workaround: Remove enhanced history interval configuration before resetting the frequency.

- CSCts70790

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

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

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

- CSCts80643

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

  A workaround is available to mitigate this vulnerability.

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

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

- CSCts85694

  Symptoms: The following error message is displayed:

  ```
  %FMANRP_ESS-3-ERREVENT: TC still has features applied. TC evsi (0x104C2E4)
  ```

  Conditions: This symptom is seen when clearing the sessions after a long time, and the memory leak increases incrementally. Leak is very slow.

  Workaround 1: Do not bring down all sessions together.

  Workaround 2: Do not tear down the sessions (scale numbers: 4k and above) together from different sources (say clearing PPP sessions and ISG sessions in lab; in field, clearing might happen via other triggers) simultaneously with no time gap between them.

  Workaround 3: Do not have accounting accuracy configured.

  Workaround 4: In this case, ISG Features are applied on TC and Session both. If we do not apply the features on the TCs, chances of this happening are less.

- CSCts97124

  Symptoms: Active crashes upon configuring a large number of TP tunnels with scale configurations either using copy paste or loading from a configuration file.

  Conditions: This symptom is not very consistent, not reproducible all the time, and happens only on adding tunnel TP configurations. The crash occurs when the protect-lsp is being configured.

  Workaround: Manually add the MPLS-TP tunnels through CLI instead of copying from a configuration or copy pasting a large configuration.

- CSCts97856

  Symptoms: PIM Assert is sent out from a router with metric [0/0], though the router has a less preferred path to reach the Source or RP.

  Conditions: This symptom occurs when an mroute is first created and its RPF lookup to the Source or RP is via BGP or Static, which involves recursive lookup, or there is no valid path to reach Source or RP. This issue only occurs in a small window in milliseconds. After the window, the metric [0/0] is corrected.

  Workaround: There is no workaround.

- CSCts97925

  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

  Conditions: This symptom is observed only with IPv6, and not with IPv4.

  Workaround: Disable IPv6 CEF.

- CSCtt01056

  Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1="", "<>", or "", then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:

  - In case of service activation from Access-Accept, the session should be terminated.
  - In case of service activation from COA, the COA should be NAKed, and the services rolled back.

  Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param="", "<>", or "". This issue is seen with service activation with a missing mandatory parameter.

  Workaround: There is no workaround.

- CSCtt02313

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

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

  Workaround: There is no workaround.

- CSCtt02645

  Symptoms: CPUHOG is seen due to flapping of all NHRP.

  Conditions: This symptom is observed with scaling to 3k spokes on RP1.

  Workaround: There is no workaround.

- CSCtt04448

  Symptoms: There is a loss of IGMP snooping entries with a traffic drop at the pmLACP PoA boxes occurring.

  Conditions: This symptom is observed when removing/re-adding member links.

  Workaround: There is no workaround.

- CSCtt11210

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

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

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

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

- CSCtt17785

  Symptoms: In the output of **show ip eigrp nei** *det*, a Cisco ASR router reports peer version for Cisco ASA devices as 0.0/0.0. Also, the Cisco ASR router does not learn any EIGRP routes redistributed on the Cisco ASA device.

  Conditions: This symptom is observed only when a Cisco ASR router is running on Cisco IOS Release 15.1(3)S and the Cisco ASA device is Cisco ASA Version 8.4(2).

  Workaround: Downgrade the Cisco ASR router to Cisco IOS Release 15.1(2)S.

- CSCtt17879

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

  Conditions: This symptom occurs:

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

  Workaround: Unconfigure and reconfigure the network backdoor.

- CSCtt26643

  Symptoms: A Cisco ASR 1006 router that is running Cisco IOS Release 15.1(2)S2 or Cisco IOS Release 15.1(3)S0a crashes with Signal 11.

  Conditions: This symptom is observed on a Cisco ASR 1006 router that is running the asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin image. The **show version** command causes the “Last reload reason: Critical software exception” error.

  Workaround: There is no workaround.

- CSCtt28703

  Symptoms: VPN client with RSA-SIG can access a profile where the CA trustpoint is not anchored.

  Conditions: This symptom is seen with the use of RSA-SIG.

  Workaround: Restrict access by using a certificate-map matching the right issuer.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 3.5/3: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:P/I:N/A:N/E:POC/RL:W/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCtt29615

  Symptoms: Any CLI command issued under af-interface mode in EIGRP router may lead to router crash.

  Conditions: This problem is observed in a Cisco router that is running Cisco IOS Release 15.2(1)S.

Workaround: There is no workaround.

- CSCtt31634

  Symptoms: Traffic drops.

  Conditions: This symptom occurs when the hw-module reloads the IM on active and posts which switchover is performed.

  Workaround: After switchover, use the **hw-module subslot reload** command to recover from the problematic state, and traffic will resume.

- CSCtt32165

  Symptoms: The Cisco Unified Border Element Enterprise on the Cisco ASR 1000 series router can fail a call with cause 47 immediately after the call connects.

  Conditions: This symptom is observed with a sufficient call volume and a call flow that redirects many calls. The Cisco ASR router can fail to provision the forwarding plane for the new call due a race condition where a prior call is not completely cleaned up on the forwarding plane before trying to use the same structure again.

  The **show voice fpi stats** command output indicates that a failure has occurred if the last column is greater than zero. For example:

  show voip fpi stats | include provisn rsp

  provisn rsp 0 32790 15

  Workaround: There is no workaround. However, Cisco IOS Release 3.4.1 is less impacted by these call failures due to a resolution of defect CSCts20058. Upgrade to Cisco IOS Release 3.4.1 until such time as this defect is resolved. In a fully redundant Cisco ASR 1006 router, you can failover the ESP slots to clear the hung entries in the forwarding plane. Other platforms will require a reload.

- CSCtt43843

  Symptoms: After reloading aggregator, PPPoE recovery is not occurring even after unshutting the dialer interface.

  Conditions: This symptom is occurring with a Cisco 7200 platform that is loaded with the Cisco IOS Interim Release 15.2(1.14)T0.1 image.

  Workaround: There is no workaround.

- CSCtt45536

  Symptoms: “FlowVar- Chunk malloc failed” messages are seen and this may be accompanied by slow console response.

  Conditions: The symptom is observed when a mix of IPv4 and IPv6 traffic is going through the router configured with QoS, VM, etc.

  Workaround: There is no workaround.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt70585

  Symptoms: IPv6 traffic is not flowing.

Conditions: This symptom is seen with IPSec v6 tunnels.

Workaround: There is no workaround.

- CSCtt95846

  Symptoms: Changing the encapsulation of an Ethernet service instance which is set up for local switching to default encapsulation may cause an error in setting up switching, resulting in an inability to switch packets.

```
PE1#show running-config | include local
connect local Ethernet0/0 1 Ethernet1/0 1
PE1#configure terminal
```

  Enter configuration commands, one per line. End with CNTL/Z.

```
PE1(config)#interface Ethernet0/0
PE1(config-if)#service instance 1 ethernet
PE1(config-if-srv)#encapsulation default
PE1(config-if-srv)#end
PE1#show ssm id
SSM Status: No switches
```

  Conditions: This symptom is observed if **no aaa new-model** is configured.

  Workaround: Unconfigure the local switching connection before changing the encapsulation of the service instance, then reconfigure the connection.

- CSCtu01172

  Symptoms: The Cisco ASR 1000 series router without an actual redundant router may crash when configured for CUBE HA based on the document “Cisco Unified Border Element High Availability(HA) on ASR platform Configuration Example.”

  Conditions: This symptom is observed with the Cisco ASR 1000 series router.

  Workaround: Remove the application configuration, that is, “no application redundancy”.

- CSCtu02286

  Symptoms: With pim-bidir in MVPN core, MVPN traffic might not flow if a PE is also a rendezvous point (RP) for the pim-bidir in core.

  Conditions: This symptom occurs with pim-bidir in MVPN core.

  Workaround: Use non pim-bidir modes.

- CSCtu12574

  Symptoms: The **show buffers** command output displays:

  1. Increased missed counters on EOBC buffers.
  2. Medium buffer leak.

```
Router#sh buffers
Buffer elements:
     779 in free list (500 max allowed)
     1582067902 hits, 0 misses, 619 created


Interface buffer pools:
....
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
```

```
00:01:17):
     273 in free list (64 min, 3000 max allowed)

EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

This DDTS tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output:

```
0A9C4ED8: 00200000 02150000 0202080B 01000000  . ............... --> IPC Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A  .T.......I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000    .R.............  --> ICC Header
            --  --
```

And, if we look at the ICC header at the underscored items 00520002:

```
0052   (represents the class name)             ----> L3_MGR_DSS_REQUESTS
0002   (represents the request name)          ----> L3_MGR_MLS_REQ
```

Workaround: Reload the system.

- CSCtu18201

  Symptoms: A Cisco router crashes due to low stack with the following display:

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

  Conditions: This symptom occurs with a low stack.

  Workaround: There is no workaround.

- CSCtu19450

  Symptoms: A system that is running Cisco IOS may reload when a large number of routes are simultaneously deleted at the same time that the inetCidrRouteTable is being walked.

  Conditions: This symptom is only likely to happen when there are large numbers of interfaces and routes within the system, and when large numbers of routes are being rapidly removed, and the system is loaded, at the same time that the inetCidrRouteTable is being walked.

  Routes may be deleted from the system both directly, and also indirectly for example, when a significant number of PPPoE sessions are removed.

  Workaround: Avoid walking the inetCidrRouteTable while significant numbers of routes are being removed from the routing system.

- CSCtu29729

  Symptoms: An attempt to create a frame-relay sub-interface on a serial interface may result in error. The serial interface can then not be configured as a frame-relay interface.

Conditions: This symptom is observed when a serial interface is configured as a multi-link frame-relay bundle link with a subsequent attempt to change the configuration to a frame-relay interface.

Workaround: There is no workaround.

- CSCtu31340

  Symptoms: The **show sip call called-number** crashes the router.

  Conditions: This symptom is observed when the call SIP state is DISCONNECT.

  Workaround: There is no workaround.

- CSCtu33956

  Symptoms: The dialer with PPP encapsulation is seen when DSL is the WAN interface. L2PT does not work.

  Conditions: This symptom is observed under the following conditions:

  – The PPPoE dialer client needs to be configured on the physical SHDSL interface.
  – The GRE tunnel destination interface should point to the dialer interface.
  – The MPLS pseudowire should go over the tunnel interface.
  – After the PPPoE session is set up, the GRE tunnel traffic gets dropped at the peer end of the PPPoE session.

  Workaround: There is no workaround.

- CSCtu35713

  Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.

  Conditions: This symptom is observed under the following conditions:

  1. Enable IPv4 address saving on BRAS.
  2. Configure AAA periodic accounting using the **aaa accounting update periodic** *time in mins* command.
  3. Initiate IPCP negotiation from the client.
  4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.

  Workaround: Configure AAA accounting with the **aaa accounting update newinfo periodic** *time in mins*.

- CSCtu36674

  Symptoms: Packets stop being transmitted in the output direction on L2transport local connect PVC on the ATM interface.

  Conditions: This symptom is observed when local connect is configured and a new ATM subinterface is configured on the same ATM main interface as the one with local connect PVC.

  Workaround 1: Perform shut/no shut on local connect.

  Workaround 2: Unconfigure/reconfigure local connect.

- CSCtu39819

  Symptoms: The Cisco ASR 1002 router configured as an RSVPAgent for Cisco Unified Communication Manager crashes under extended traffic.

Conditions: This symptom is observed on a Cisco ASR 1002 router configured as an RSVPAgent for CUCM End-to-End RSVP feature. The router crashes after 45 minutes of traffic run with 150 simultaneous up MTP-RSVP sessions.

The asr1000rp1-adventerprisek9.03.04.00a.S.151-3.S0a.bin image is used.

Workaround: There is no workaround.

- CSCtu41137

  Symptoms: IOSD Core@fib_table_find_exact_match is seen while unconfiguring tunnel interface.

  Conditions: The core is observed while doing unconfiguration.

  Workaround: There is no workaround.

- CSCtu43731

  Symptoms: On an RP1, RP switchover causes an RP reset.

  Conditions: This symptom is observed with RP switchover under the following conditions:

  – The router must be an RP1

  – The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.

  An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.

  Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.

  Workaround 2: Do not enable FNF monitoring.

- CSCtu87383

  Symptoms: CFM global configuration does not get applied to LC slots that are greater than 20 on LC OIR. This problem is specific to CPT platform where satellite box slot numbers go from 36 to 55.

  Conditions: This symptom occurs with satellite box OIR.

  Workaround: Disable and reenable CFM global configuration.

- CSCtu89771

  Symptoms: The Cisco ASR 1000 series router RP crashes while unconfiguring or removing the **no area 0 authentication ipsec spi <>** command.

  This behavior is not observed at the first few instances of unconfiguring the above CLI.

  Conditions: This symptom is observed only in automated tests where unconfiguring the authentication with the above CLI is executed multiple (approximately 3) times on the Cisco ASR 1000 series router. This leads to the RP crashes.

  Workaround: There is no workaround.

- CSCtu92213

  Symptoms: Console is stuck and irresponsive.

  Conditions: This symptom is seen when EVC with QoS is scaled, and traffic is being sent through many policy-maps with a large queue limit.

  Workaround: Configure a smaller queue-limit under each class on all egress policy-maps in use.

- CSCtu92289

  Symptoms: VCCV BFD on PW HE (routed pseudowire) is not working.

Conditions: VCCV BFD is not working on routed pseudowire but works fine on scalable EoMPLS.

Workaround: There is no workaround.

- CSCtu92673

  Symptoms: L2TP tunnels are not getting established with PPPoE relay.

  Conditions: This issue is seen on a Cisco 7200 router that is running Cisco IOS Interim Release 15.2(01.12)S.

  Workaround: There is no workaround.

- CSCtv19529

  Symptoms: Router crashes on unconfiguring the last available DHCP pool. Crash will also be seen on running the **no service dhcp**.

  Conditions: This crash can happen only if "DHCP Client" process is running on the router along with the DHCP relay processes (DHCPD Receive, DHCPD Timer, DHCPD Database).

  The client process can be started:

  1. from an DHCP autoinstall attempt during router startup (with no nvram config).
  2. if the **ip address dhcp** is run on one of the interfaces. 3) if the router was used for DHCP proxy client operations.

  The relay processes are started when a DHCP pool is created by the **ip dhcp pool** *pool* command.

  Workaround: Have a dummy DHCP pool created using the **ip dhcp pool** *dummy_pool* command, and never delete this pool. Other pools can be created and removed at will, the *dummy_pool* should not be removed. In addition, do not execute the **no service dhcp** command.

- CSCtw43640

  Symptoms: An IP ping/CFM session through Handoff FPGA fails.

  Conditions: This symptom is observed after switchover with IM in slot 5.

  Workaround: There is no workaround.

- CSCtw45055

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

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

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

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

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

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

Workaround: There is no workaround.

- CSCtw45168

  Symptoms: DTMF interworking fails when MTP is used to convert OOB---RFC2833 and vice versa.

  Conditions: This symptom is observed when MTP is used to convert OOB---RFC2833 and vice versa. This issue is seen starting from Cisco IOS XE Release 3.2S. Cisco IOS XE Release 3.1S should work fine.

  Workaround: There is no workaround.

- CSCtw46625

  Symptoms: The QL value is DNU although the four least significant bits of SSM S1 byte are pointing to PRC (bits: 0010).

  Conditions: This symptom is observed when SSM S1 byte is received on CEoPs SPAs or channelized SPA-1XCHSTM1/OC3.

  Workaround: Force the QL PRC value by executing the following command:

  network-clock quality-level rx QL-PRC *controller SONET 1/2/0*

- CSCtw48209

  Symptoms: High-end Cisco devices running Cisco IOS are likely affected. Active features at the time of this problem manifestation include any condition that leads to RSVP SNMP notification generation in Cisco IOS. BGP/MPLS TE instability, leading to changes to RSVP session status change, is observed in a test scenario while running Cisco IOS Release SXI4 and Cisco IOS Release SXI7. The issue is not reproducible consistently.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SXI4, Cisco IOS Release 12.2(33)SXI7, Cisco IOS Release 12.2SR, Cisco IOS Release 12.2SX, and Cisco IOS Release 15S.

  Workaround: Disable RSVP notification using the **no snmp-server enable traps rsvp** command.

- CSCtw50277

  Symptoms: Policy manager is getting apply config failed on standby while policy is activated through CoA. The router later crashes in policy code.

  Conditions: This symptom is seen when CoA activated policy install is failing on standby RP.

  Workaround: There is no workaround.

- CSCtw51134

  Symptoms: IMA interface configuration is lost post stateful switchover (SSO).

  Conditions: This symptom occurs after SSO.

  Workaround: There is no workaround.

- CSCtw52504

  Symptoms: WAN mode is not enabled on 10G IMs.

  Conditions: This symptom is observed when a 10G IM operates in LAN mode by default. The WAN mode supports SONET alarms to interface with SONET-like equipments.

  Workaround: There is no workaround.

- CSCtw52610

  Symptoms: Some of the TCes will switch to fallback interface, and the remaining TCes on primary interface will be in OOP state.

  Conditions: The issue is seen when primary link is considered OOP based on utilization despite using the **no resolve utilization** command.

  Workaround: There is no workaround if PfR policy with and without utilization is needed. If PfR policy based on utilization is not needed, then configure “max-xmit-utilization percentage 100”.

- CSCtw58395

  Symptoms: When executing the **clear crypto session** command in 4k FlexVPN cases, the memory of crypto IKEv2 is increasing.

  Conditions: This symptom is observed when the session is flapping.

  Workaround: There is no workaround.

- CSCtw58586

  Symptoms: IKEv2 CLI configuration currently requires to manually link the crypto IKEv2 profile default to the crypto IPSec profile default. This enhancement request will change the behavior and create an automatic anchorage.

  Conditions: This symptom is seen in IKEv2 usage.

  Workaround: There is no workaround.

- CSCtw64040

  Symptoms: Crash due to MPLS, which appears to be associated with load- balancing.

  Conditions: This symptom occurs when MPLS is configured.

  Workaround: There is no workaround.

- CSCtw68745

  Symptoms: A Cisco ASR 1000 router acting as DHPCv6 Relay standby crashes when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.

  Conditions: This symptom occurs when there is high DHCPv6 incoming traffic and if DHCPv6 relay is configured on many (around 5k) interfaces.

  Workaround: There is no workaround.

- CSCtw73551

  Symptoms: Standby RP can crash due to a memory leak processing calls. The crashinfo file identifies the process as follows:

  ```
  UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps
  ```

  Conditions: This symptom is seen on CUBE enterprise on the Cisco ASR 1000 series router with redundant RPs and approximately 2.4 million calls processed from last start of the standby RP.

  Workaround: There is no workaround.

- CSCtw76044

  Symptoms: Need IGMP/MLD information to make IGMP/MLP snooping work.

  Conditions: The symptom is observed under all conditions.

  Workaround: There is no workaround.

- CSCtw79579

  Symptoms: Standby fails to be in standby HOT state after reload.

Conditions: This symptom is seen after removal of an IM and doing RSP stateful switchover (SSO) and then trying to bring up the standby RSP.

Workaround: There is no workaround.

- CSCtw85883

  Symptoms: The error “ace_add_one_map failed” occurs while adding an ACE to a crypto ACL that is being used by a crypto map.

  Conditions: This symptom is observed when the crypto map is applied to an interface and the crypto ACL being modified is also in use.

  Workaround: Remove the crypto map and apply the ACL changes to avoid the error.

- CSCtw94319

  Symptoms: Crash is seen at dhcpd_forward_request.

  Conditions: This symptom is seen when the IP DHCP Relay feature is used in scaled configuration.

  Workaround: Remove the **ip dhcp relay information option vpn** command, if possible. Otherwise, there is no workaround.

- CSCtw99290

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

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

  Workaround: There is no workaround.

- CSCtw99877

  Symptoms: IOMD process on 10G IM crashes upon booting standby.

  Conditions: This symptom is observed when the interface state is down on active.

  Workaround: There is no workaround.

- CSCtx01604

  Symptoms: Cisco IOS might crash on some 64-bit platform if CNS ID is configured as the IP address of some active network interface, and this IP address is changed in the middle of some critical CNS feature operations.

  Conditions: This problem presents a bad planning of bootstrapping a Cisco IOS device via an unreliable network interface whose IP address could be changed any time during the bootstrapping.

  Workaround: Do not use any dynamic network interface IP address as CNS ID.

- CSCtx05942

  Symptoms: The session to the service module from the Supervisor Fails. This can happen with SAMI, NAM, NAM-2 etc. modules.

  For example, if the SAMI card is in Slot 2, the **session slot** *2* **processor 0** command fails to create a telnet session and fails to give out the following messages:

```
SUP#session slot 2 proc 3
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.33 ...
```

```
% Connection timed out; remote host not responding
```

Conditions: This symptom occurs with Cisco IOS Release 15.2(1)S release. It is not observed with Cisco IOS Release 15.1(3)S1 or lower version.

Workaround: Downgrading the Supervisor to Cisco IOS Release 15.1(3)S1 or lower version resolves this issue.

- CSCtx09614

  Symptoms: With the preconfigured ATM configuration, the standby RSP does not boot up.

  Conditions: This symptom is observed when one of the RSPs is up and the running configuration has the ATM configuration under the controller.

  Workaround: There is no workaround. Without an ATM configuration, the standby RSP goes to standby mode.

- CSCtx21206

  Symptoms: BFDv6 hardware offloaded sessions do not come up with all IPv6 source addresses.

  Conditions: This symptom is observed with interface source IPv6 addresses that have some specific bits in the 6th byte set like 6001:1:C::1..

  Workaround: Reconfigure the source IPv6 addresses to some address that will not match the criteria mentioned in the above Conditions.

- CSCtx29543

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

  Conditions: This symptom occurs under the following conditions:

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

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

  Workaround: There are two possible workarounds:

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

- CSCtx63034

  Symptoms: After a Cisco 7600 router is powered by PWR-2500-DC, PWR-4000-DC or PWR-6000-DC to Cisco IOS Release 15.2(1)S, the router logs the following error messages:

  ```
  %C7600_PWR-SP-3-PSUNKNOWN: Unknown power supply in slot 1 (idprom read
  failed).
  %OIR-SP-6-INSPS: Power supply inserted in slot 1
  %C7600_PWR-SP-4-PSOK: power supply 1 turned on.
  ```

  The **show power** command shows that the power supply only provides 919W. Most of the line cards cannot be powered up.

  Conditions: This symptom is observed in Cisco IOS Release 15.2(1)S only. The problem does not occur in Cisco IOS Release 15.1(3)S1. PWR-4000-DC and PWR-6000-DC are confirmed to be affected by this problem.

Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 15.2(1)S

This section describes possibly unexpected behavior by Cisco IOS Release 15.2(1)S. All the caveats listed in this section are open in Cisco IOS Release 15.2(1)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtg68047

  Symptoms: The router reloads.

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

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

- CSCtj58706

  Symptoms: On executing ISSU runversion, the standby RP reloads multiple times before reaching hot-standby.

  Conditions: This symptom is observed during ISSU upgrade/downgrade with the iso1-iso2 image. This issue is seen with scaled configuration of 7000 L2VPN, 300 BGP, 300 EIGRP, and 8000 EVC sessions.

  Workaround: There is no workaround.

- CSCtk62763

  Symptoms: A Cisco 7600 router equipped with multiple DFC line cards may experience an unexpected reload because of increased IGMP activity.

  Conditions: This symptom is observed when IGMP joins and leaves (OIF churn) at approximately 160pps or more on DFCs with around 600 mroutes that have SVIs as OIFs.

  Workaround: There is no workaround.

- CSCtn83900

  Symptoms: After performing legacy mode or native mode subpackage ISSU with flexible NetFlow configured, the interface to monitor bindings may not be present on the newly active RP.

  Conditions: This symptom is observed when a legacy mode or native mode subpackage ISSU is performed with FNF configured.

  Workaround: Remove the FNF monitors prior to the subpackage ISSU. Add the monitors back to the interface configuration after the upgrade. Alternatively, use super-package ISSU, which does not have this limitation.

- CSCto71671

  Symptoms: Using the **radius-server source-ports extended** command does not increase AAA requests source UDP ports as expected when Radius.ID has wrapped over, causing duplicate (dropped) requests on Radius, and forcing the Cisco ASR 1000 router to time out and retransmit.

  Conditions: This symptom is observed with a high AAA requests rate, and/or slow Radius response time, leading to a number of outstanding requests greater than 255.

  Workaround: There is no workaround.

- CSCtq80891

  Symptoms: The Processor Pool for the Cisco IOS memory is used up with most of the buffers in the "IPv6 PIM input queue".

  Conditions: This symptom is observed with the following topology:

  IXIA [IPv6 Mcast Source] ------ TR1 (ASR1k) ------|500 IPv6 over IPv4 GRE

  Tunnels | ------ UUT (ASR1k) [IPv6 RP] ------ |500 IPv6 over IPv4 GRE

  Tunnels | ------ TR2 (7200) ------ IXIA [IPv6 Mcast MLD Hosts]

  - 500 IPv6 Sources sending Mcast traffic to 500 IPv6 Mcast groups
  - 500 PIM-RP on UUT
  - 500 PIM-RP Acl to make sure 1 Mcast-group/Tunnel
  - The GRE tunnels could be configured with tunnel protection or not.

  The reproduce procedure is as follows:

  1. Copy configurations (IPv6 over IPv4 GRE Tunnel Protections and IPv6 Mcast included) to TR1, TR2, and UUT.
  2. Launch Mcast traffic (500M) on IXIA.
  3. Hit the Cisco IOS memory depletion issue on UUT.

  Workaround: Configure the punt policer for PIM register packets as follows:

  platform punt-policer 55 limit-number
  platform punt-policer 55 limit-number high

  The limit-number above is a number between 1000-2000.

- CSCtr80274

  Symptoms: CISCO-LICENSE-MGMT-MIB does not populate.

  Conditions: This symptom occurs when the required license is installed on the Cisco ASR 903 router, but the SNMP query does not return any value.

```
NMS-RACK1-RUDY-1#show license
Index 1 Feature: metroaggrservices
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: metroipservices
        Period left: 8  weeks 4  days
        License Type: Evaluation
        License State: Active, Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None
Index 3 Feature: metroservices
        Period left: 8  weeks 4  days
        License Type: Evaluation
        License State: Active, Not in Use, EULA not accepted
        License Count: Non-Counted
```

```
        License Priority: None
sw-mrrbu-nms-2:2> getmany 3.3.2.11 ciscoLicenseMgmtMIB
sw-mrrbu-nms-2:3>
```

Workaround: There is no workaround.

- CSCts05124

  Symptoms: A zero-byte crash file is generated upon a crash with TREX SPA.

  Conditions: This symptom is observed with a test crash on a SIP-400 line card with TREX SPA inserted.

  Workaround: There is no workaround.

- CSCts11715

  Symptoms: After shutting the tunnel, ISAKMP does not turn OFF.

  Conditions: This symptom is observed in a scaled DMVPN setup with more than 1k spokes.

  Workaround: There is no workaround.

- CSCts12499

  Symptoms: SPA firmware crash at one bay leads to SPA crash in another bay.

  Conditions: This symptom is observed when “test crash cema” is executed from the SPA console. leading to the SPA in the other bay to reload. Also, the crashinfo is not present in the RP disk.

  Workaround: There is no workaround.

- CSCts13255

  Symptoms: Standby SUP crash is observed on the Cisco 7609 router after upgrade to c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is random and recurring. Tracebacks are generated with the following error message:

  ```
  %CPU_MONITOR-STDBY-3-PEER_FAILED: CPU_MONITOR peer process has failed to receive
  heartbeats
  ```

  Conditions: This symptom is observed on the Cisco 7609 router after upgrade to c7600s72033-advipservicesk9-mz.150-1.S3a.bin. This issue is also seen with Cisco IOS Release 12.2(33)SRE.

  Workaround: There is no workaround.

- CSCts20632

  Symptoms: If subclassification and classification for the protocol is configured in a different class map, configuring the port map and assigning a different port (other than 80) for HTTP causes unexpected error messages to be displayed.

  Conditions: This symptom is observed when subclassification and protocol classification is configured for HTTP and a port map is configured for HTTP.

  Workaround: There is no workaround.

- CSCts47550

  Symptoms: When applying protocol attributes policy rules, traceback may be seen.

  Conditions: This symptom is not consistent and may or may not appear when applying the protocol attributes policy rules. The symptom is also not consistent with a specific protocol, but may appear with respect to different protocols.

  Workaround: There is no workaround.

- CSCts63426

  Symptoms: With 1K EoMPLS PWs, 6 percent performance drop is observed in Cisco IOS XE Release 3.5 compared to Cisco IOS XE Release 3.4 performance.

  Conditions: This symptom is observed with 1K EoMPLS PWs in Cisco IOS XE Release 3.5.

  Workaround: There is no workaround.

- CSCts63658

  Symptoms: Multicast traffic do not flow over EVCs on the port-channel.

  Conditions: This symptom is observed during router reload.

  Workaround: Reconfigure after the router reload. Configure regular EFPs before EFPs on the PC in the same BD.

- CSCts82598

  Symptoms: Incorrect IP from the NAT pool is chosen for translation, when one protocol exhausts all ports of all IPs and another protocol traffic is received.

  Conditions: This symptom occurs when one protocol (for example, TCP) exhausts all ports of all IPs in a pool, and only one IP from the pool is selected for translation, thus limiting the capacity of creating translations. This happens only when one protocol completely exhausts all ports and then another protocol traffic starts. This usually is not the case in customer environments that mostly see both TCP and UDP traffic hitting the box time.

  Workaround: There is no workaround.

- CSCts97925

  Symptoms: IPv6 pings within VRF fail, where the next-hop (egress) is part of the global.

  Conditions: This symptom is observed only with IPv6, and not with IPv4.

  Workaround: Disable IPv6 CEF.

- CSCtt01056

  Symptoms: When a shell map configuration includes a parameter with no default value, that is, parameter1=””, “<>”, or ““, then that parameter should be considered mandatory. During service activation of that shell map, if parameter1 is not provided by Radius, the activation should be rejected:

  - In case of service activation from Access-Accept, the session should be terminated. - In case of service activation from COA, the COA should be NAKed, and the services rolled back.

  Conditions: This symptom is observed with a shell map configuration when some parameters do not have the default value configured, such as param=””, “<>”, or ““. This issue is seen with service activation with a missing mandatory parameter.

  Workaround: There is no workaround.

- CSCtt02645

  Symptoms: CPUHOG is seen due to flapping of all NHRP.

  Conditions: This symptom is observed with scaling to 3k spokes on RP1.

  Workaround: There is no workaround.

- CSCtt04724

  Symptoms: On PPPoEoX, when activating multiple services from Access-Accept with long Cisco-SSG-Account-Info strings, if the aggregated string length exceeds the current limit of 256 characters, then the service activation fails, a traceback is seen, and the session is allowed to establish, no services will be applied in the ingress and/or egress directions.

  Conditions: This symptom is observed when the aggregated services string length exceeds the limit (256 characters).

  Workaround: The session should be terminated instead. In case of service activation from CoA, if the cumulative services string length exceeds the limit, then the last CoA should be NAKed, and the services rolled back to the previous state.

- CSCtt11210

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

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

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

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

- CSCtt11558

  Symptoms: The Cisco ASR 1000 router displays the “INVALID_GPM_ACCESS” error message due to invalid GPM load. This may cause unexpected Embedded Services Processors (ESP) reload.

  Conditions: This symptom is observed when a small packet is sent from a BDI interface to an Ethernet service instance with either the **rewrite egress tag** command or the **rewrite ingress tag** command with the **symmetric** option present.

  Workaround: There is no workaround.

- CSCtt21257

  Symptoms: After a reload or switchover, all interfaces on one or more IMs may be down down. The state of the IMs is “ok, active”, which is shown in the **show platform** command output.

  Conditions: This symptom is occasionally observed after a reload or a switchover.

  Workaround: Power cycle the box.

- CSCtt26532

  Symptoms: With QoS policy-map configured on a BFD interface, modifying the QoS policy-map flaps the BFD session.

  Conditions: This symptom is observed when BFD and QoS policy-maps are configured on the same interface.

  Workaround: There is no workaround.

  Further Problem Description: QoS and BFD use a common flag that gets reset and set during QoS policy-map update, causing the BFD session to flap. BFD session flap leads to the OSPF session also going down.

- CSCtt33937

  Symptoms: Configure port 7 on the Gigabit IM as a port to forward traffic using IP routing.

  ```
  config t
  interface g0/0/7
  ```

```
ip address 10.0.0.1 255.255.255.0
```

Conditions: This symptom is observed when traffic is flowing well. When you perform a switchover, and once the standby becomes the new active, the traffic does not hit the ingress counter of the interface itself. On checking the links status using the registers, the SGMI link appears out of sync.

Workaround: There is no workaround. Reload the box when this symptom is observed.

- CSCtt34361

  Symptoms: During a soak test with 1800 PPPoE sessions flapping with the IPv4 Saving feature enabled + per-user ACLv4 and ACLv6, there is no ISG service. After 56 iterations, one memory snapshot is taken every four iterations, that is, roughly 270 seconds per iteration. The test duration is 4 hours, with total 100800 sessions established with an average of 7cps.

  Conditions: This symptom occurs under the following conditions:

  1. No active session is there in the router.
  2. Establish 1800 PTA dual-stack sessions with per-user ACL from Radius + IPV4 Saving feature.
  3. Wait till all sessions come UP.
  4. Take a memory leak snapshot “high”.
  5. Wait for all sessions to time out on the Idle timer (no traffic).
  6. Wait for all sessions to go DOWN.
  7. Take a memory snapshot.
  8. Loop back to 1.

  Workaround: There is no workaround.

- CSCtt45654

  Symptoms: In a DVTI IPSec + NAT-t scaling case, when doing session flapping continually, several Virtual-Access interfaces are “protocol down” and are not deleted.

  Conditions: This symptom can be observed in a DVTI IPSec + NAT-t scenario when session flapping is done in the spoke side.

  Workaround: There is no workaround.

- CSCtt45801

  Symptoms: The DMVPN HUB RP crashes with the default EIGRP timer when scaling to 4k spokes.

  Conditions: This symptom occurs when scaling to 4k spokes.

  Workaround: Changing the EIGRP timer to longer may reduce the chances of a crash.

- CSCtt70133

  Symptoms: The RP resets with FlexVPN configuration.

  Conditions: This symptom is observed when using the **clear crypto session** command on the console.

  Workaround: There is no workaround.

- CSCtt70346

  Symptoms: IOMD crash is seen when running the PTP session.

  Conditions: This symptom is observed when running the PTP session for a long time. Sometimes, this issue is seen when changing PTP packet rates. This issue is seen rarely.

  Workaround: There is no workaround.

- CSCtt70498

  Symptoms: After a reload or switchover, the state of F0 or F1 may become “disconnecting” instead of “ok, active/standby”, which is shown in the **show platform** command output. As a result, the corresponding RSP does not forward traffic.

  Conditions: This symptom is occasionally observed after a reload or a switchover.

  Workaround: Power cycle the box.

- CSCtt94147

  Symptoms: Nile manager crash is observed.

  Conditions: This symptom is observed with the following conditions:

  - VPLS in the core.
  - REP in the access.
  - The access-side REP segment flaps a few times.

  Workaround: There is no workaround.

- CSCtt94566

  Symptoms: The router crashes before all sessions come up.

  Conditions: This symptom occurs before all sessions come up.

  Workaround: There is no workaround.

- CSCtt95577

  Symptoms: After creating the 994th VC on a T1/E1 IM on Rudy, the traffic flow stops. Packets get dropped on the egress on Rudy.

  Conditions: This symptom is observed when ping starts to fail on all the pre-existing VCs upon adding the 994th VC. The working is unaffected till 993 VCs.

  Workaround: Delete the 994th VC to make the pre-existing VCs forward traffic.

- CSCtt97164

  Symptoms: If the router interface is flapped, the HSRP message may be dropped by the punt/inject path.

  Conditions: This symptom is seen if the router interface is flapped.

  Workaround: Disable the inject bypass.

- CSCtt97473

  Symptoms: After a reload or switchover, the RSP may reset during bootup.

  Conditions: This symptom is observed occasionally after a reload or switchover.

  Workaround: There is no workaround.

- CSCtt98574

  Symptoms: After a reload or switchover, the state of one or more IMs may become “out of service” instead of “ok, active/standby”, which is shown in the **show platform** command output. As a result, the corresponding interfaces do not come up.

  Conditions: This symptom is occasionally observed after a reload or a switchover.

  Workaround: Power cycle the box.

- CSCtt99235

  Symptoms: After a switchover, an IOMD process crashes because it has failed to establish LIPC connection.

  Conditions: This symptom is seen occasionally after a switchover.

  Workaround: Reload the box.

- CSCtu02280

  Symptoms: When running the PTP session for more than 12 hours, PTPD may crash.

  Conditions: This symptom occurs when running the PTP session for a long time.

  Workaround: There is no workaround.

- CSCtu02476

  Symptoms: An SSO followed by a change in the xconnect MTU results in the pseudowire in the redundant RP to go down. The pseudowire in the Active RP remains up and running. A subsequent SSO results in the pseudowire to go down.

  Conditions: This symptom is observed with “encapsulation default” at that end of the pseudowire where SSO is performed. An SSO followed by a change in the MTU value, and then a subsequent SSO, causes the pseudowire to go down. This issue is also seen in a setup with redundant pseudowires, where the primary and backup pseudowires configured under the service instance do not come up after changing the MTU with SSO.

  Workaround: Execute “no xconnect” under the service instance, and then reconfigure the pseudowire with the new MTU value under the service instance.

- CSCtu03699

  Symptoms: The Nile Manager crashes.

  Conditions: This symptom is observed when reloading the TP tunnel endpoint multiple times.

  Workaround: There is no workaround.

- CSCtu12574

  Symptoms: The **show buffers** command output displays:

  1. Increased missed counters on EOBC buffers.
  2. Medium buffer leak.

```
Router#sh buffers
Buffer elements:
     779 in free list (500 max allowed)
     1582067902 hits, 0 misses, 619 created
Interface buffer pools:
....
Medium buffers, 256 bytes (total 89647, permanent 3000, peak 89647 @
00:01:17):
     273 in free list (64 min, 3000 max allowed)
EOBC0/0 buffers, 1524 bytes (total 2400, permanent 2400):
     0 in free list (0 min, 2400 max allowed)
     2400 hits, 161836 fallbacks
     1200 max cache size, 129 in cache
....
```

The leak is small. It is a leak of 64 bytes per buffer that is leaked, and the leak appears to be very slow.

Conditions: The **show buffers old** command output displays some buffers hanging on the EOBC buffers list for a really long time, such as weeks or even more. This issue is a corner case and the buffer leak rate is slow.

The DDTS CSCtr34960 tracks the leak specific to IPC application l3-mgr.

From the **show buffers old pack** output:

```
0A9C4ED8: 00200000 02150000 0202080B 01000000  . ..............    -----> IPC
Header
0A9C4EE8: 97D49493 00081608 03493E4D 06927C9A  .T.......I>M..|.
0A9C4EF8: 00520002 00000000 00000000 000000    .R.............       ------>
ICC Header
            --  --
```

And, if we look at the ICC header at the underscored items 00520002:

```
0052   (represents the class name)             ----> L3_MGR_DSS_REQUESTS
0002   (represents the request name)          ----> L3_MGR_MLS_REQ
```

Workaround: Reload the system.

- CSCtu13806

  Symptoms: Upon switchover, the “red_switchover_process” process causes a crash on the old active RSP.

  Conditions: This symptom is observed upon switchover.

  Workaround: This crash is harmless as another RSP becomes active and works properly. Reboot the RSP to make it come up as standby.

- CSCtu13951

  Symptoms: Pending objects appear on the active and standby ESP.

  Conditions: This symptom occurs when the edge device to the core link is flapped multiple times for close to two days.

  Workaround: There is no workaround.

- CSCtu17006

  Symptoms: Mediatrace is not working because RSVP fails to select the output interface.

  Conditions: This symptom is observed only with PFR configuration.

  Workaround: Remove the PFR configuration.

- CSCtu17296

  Symptoms: Traffic failure occurs on 3 to 4 VLANs out of 1000.

  Conditions: This symptom is observed after reloading the UUT.

  Workaround: Remove and readd the service instance configuration for the affected VLANs.

- CSCtu17540

  Symptoms: IOMD core is generated on switchover for T1/E1 IM. After switchover, the IOMD process is aborted.

  Conditions: This symptom is observed with every switchover.

  Workaround: There is no workaround.

- CSCtu18150

  Symptoms: FP crash occurs due to a wrong FCID handling issue.

  Conditions: This symptom occurs due to a wrong FCID handling issue.

  Workaround: There is no workaround.

- CSCtu24765

  Symptoms: Under scale (28.8K PPPoX sessions), when executing “show policy-map session” from the CLI, both ESPs crash.

  Conditions: This symptom is observed with a large scale, that is, 28K PPPoE sessions established + ISG QoS services.

  Workaround: There is no workaround.

- CSCtu27601

  Symptoms: On ATM BRAS under scale (16K PPPPoEOA sessions + ISG services), the ESP crashes occasionally during sessions establishment.

  Conditions: This symptom is observed with a large scale (16K PPPPoEOA sessions + services).

  Workaround: There is no workaround.

- CSCtu28990

  Symptoms: RP crash is observed at SYS-6-STACKLOW: Stack for process XDR Mcast.

  Conditions: This symptom is observed when performing shut/no shut on interfaces on a configuration-rich system.

  Workaround: There is no workaround.

- CSCtu29047

  Symptoms: After a reload or switchover, the RSP may exhibit a kernel hang.

  Conditions: This symptom is observed occasionally after a reload or switchover.

  Workaround: Power cycle the box.

- CSCtu32913

  Symptoms: The system may crash when NBAR is continuously enabled/disabled.

  Conditions: This symptom is observed when NBAR is continuously enabled/disabled. This issue is seen after more than 12 hours of continuously enabling/disabling NBAR under traffic.

  Workaround: There is no workaround. The system works fine after reload.

- CSCtu32935

  Symptoms: IPv6 traffic loss of around 30 seconds is seen for routes learned from dynamic routing protocols upon RSP switchover with the Nonstop Forwarding (NSF) configuration. IPv6 CEF is not programmed on the standby RSP.

  Conditions: This symptom is observed with RSP switchover.

  Workaround: There is no workaround for the dynamic routing protocol. Problem will not be seen for static route.

- CSCtu33258

  Symptoms: LDP over MPLS-TP tunnel fails to get established upon router reload.

  Conditions: This symptom is seldom seen when the router is reloaded with scaled MPLS-TP tunnels that have LDP session established over the tunnels. Pinging traffic through the tunnel fails.

Workaround: There is no workaround.

- CSCtu34906

  Symptoms: All ptp sessions go down on the BC upon configuring more than 63 slaves to negotiate with it.

  Conditions: This symptom is observed on the BC when there are more than 63 slaves trying to negotiate with the master. This issue is not seen with lesser number of slaves. It was verified that the sessions are stable with 62 slaves. This issue is also not seen with the OC master, but only with the BC master.

  Workaround: This issue is not seen with lesser number of slaves. It was verified that the sessions are stable with 62 slaves. This issue is also not seen with the OC master.

- CSCtu35713

  Symptoms: IPv4 address saving: IPCP state change does not trigger session accounting update.

  Conditions: This symptom is observed under the following conditions:

  1. Enable IPv4 address saving on BRAS.
  2. Configure AAA periodic accounting using the **aaa accounting update periodic** *time in mins* command.
  3. Initiate IPCP negotiation from the client.
  4. After IPCP negotiation is complete, BRAS does not send an interim accounting update containing IPv4 address save VSA and the new IPv4 address assigned to the client.

  Workaround: Configure AAA accounting with the **aaa accounting update newinfo periodic** *time in mins* command.

- CSCtu41497

  Symptoms: The Nile Manager crashes.

  Conditions: This symptom is observed with a 256 rmep scale.

  Workaround: There is no workaround.

- CSCtu43120

  Symptoms: Service accounting start is not sent for L2TP sessions.

  Conditions: This symptom is observed with L2TP.

  Workaround: There is no workaround.

- CSCtu43731

  Symptoms: On an RP1, RP switchover causes an RP reset.

  Conditions: This symptom is observed with RP switchover under the following conditions:

  - The router must be an RP1.
  - The configuration of Flexible NetFlow (FNF) or equivalent must be applied to 4000 or more interfaces. In this case of testing, 4000 DVTI interfaces were in use.

  An equivalent of FNF is AVC or passive Video Monitoring. That is, those configured on a comparable number of interfaces will have the same effect.

  Workaround 1: Prior to doing a controlled switchover, such as ISSU, deconfigure FNF from some interfaces to take it well under the threshold at which the issue can occur.

  Workaround 2: Do not enable FNF monitoring.

- CSCtu53275

  Symptoms: Out to in traffic is not handled properly. The lookup on inside global is only done in the global routing table and not in the VRF routing table.

  Conditions: This symptom is observed with the following configuration on the Cisco ASR 1000 series router:

  ```
  ip nat inside source static 1.1.1.1 1.1.1.1 vrf test-pe1
  ```

  In to out traffic is handled properly.

  Workaround: A static route in the global routing table for each of these addresses (assuming they are unique) should provide a workaround for this issue.

- CSCtu98727

  Symptoms: ANCP shaping with Model F fails with BRR classes.

  Conditions: This symptom is observed with BRR classes, but works fine with LLQ (priority level) classes.

  Workaround: There is no workaround.

- CSCtv22685

  Symptoms: The ESP on the Cisco ASR 1000 router crashes or the GRE tunnel does not switch over when the destination interface is removed or the route changes, causing the tunnel interface to stop forwarding packets.

  Conditions: This symptom is observed when multiple GRE tunnels are configured on the same interface(s) with a high traffic rate across the tunnels.

  Workaround: Only configure one GRE tunnel per physical interface.

Resolved Caveats—Cisco IOS Release 15.2(1)S

All the caveats listed in this section are resolved in Cisco IOS Release 15.2(1)S. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCtj33003

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

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

  This advisory is available at the following link:

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

- CSCtr28857

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

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

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

- CSCts80643

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

  A workaround is available to mitigate this vulnerability.

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

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