Caveats for Cisco IOS Release 15.2(2)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:

- Open Caveats—Cisco IOS Release 15.2(2)S2, page 251
- Resolved Caveats—Cisco IOS Release 15.2(2)S2, page 251
- Resolved Caveats—Cisco IOS Release 15.2(2)S1, page 280
- Open Caveats—Cisco IOS Release 15.2(2)S, page 295
- Resolved Caveats—Cisco IOS Release 15.2(2)S, page 297

Open Caveats—Cisco IOS Release 15.2(2)S2

This section describes possibly unexpected behavior by Cisco IOS Release 15.2(2)S2. All the caveats listed in this section are open in Cisco IOS Release 15.2(2)S2. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCty54695

  Symptoms: RRI routes are missing when IPsec SA is up after peer IP change.

  Conditions: This symptom is observed under the following conditions:

  - Cisco ASR 1002 router running Cisco IOS XE Release 3.4.2S.
  - Dynamic crypto map with RRI.
  - Peer changes the IP address frequently.

  Workaround: Clear the crypto session with the peer.

Resolved Caveats—Cisco IOS Release 15.2(2)S2

Cisco IOS Release 15.2(2)S2 is a rebuild release for Cisco IOS Release 15.2(2)S. The caveats in this section are resolved in Cisco IOS Release 15.2(2)S2 but may be open in previous Cisco IOS releases.

- CSCsi46463

  Symptoms: A VRF-aware Name Server may not source its addresses from a VRF interface but, instead, from global interface that is connected to the Name Server.

  Conditions: This symptom is observed on a Cisco router that functions as a Name Server and that has the VRF-Aware DNS feature enabled.

  Workaround: Ping the Name Server from a CE router.

- CSCtg47129

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

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

  This advisory is available at the following link:

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

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

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

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

- CSCtj93356

  Symptoms: Batch suspending from platform causes the MFIB on the line card to go into reloading state.

  Conditions: This symptom occurs when MFIB on the line card goes into reloading state and then finally to purge state after removal/addition of MVRFs is done followed by a line card reset.

  Workaround: There is no workaround.

- CSCtr42806

  Symptoms: The following error message can be seen sometimes, when standby or a line card is coming UP:

  ```
  %TID_HA-3-ISSU_ERR: TABLEID-ISSU-RP: FAILED: Negotiation start:
  ISSU_RC_CLIENT_ENTITY_DOES_NOT_EXIST_IN_PEER
  ```

  Conditions: This symptom occurs occasionally at standby/line card bootup.

  Workaround: There is no workaround.

- CSCts55778

  Symptoms: This is a problem involving two SAF forwarders, where one is running EIGRP rel8/Service-Routing rel1 and the other is running EIGRP dev9/Service-Routing dev2. The capabilities-manager, a client of the service-routing infrastructure, will advertise two services. When forwarders are peering with the same release image, the services propagate between the forwarders without any problems. But, when you run rel8/rel1 on one forwarder, and dev9/dev2 on the other forwarder, a third service appears in the topology table and the SR database that was not advertised. Note: The problem cannot be recreated if both forwarders are running an Cisco IOS XE Release 3.4S or and Cisco IOS XE Release 3.5S image.

Conditions: This symptom occurs if two SAF forwarders peer with each other, where one SAF forwarder is running EIGRP SAF rel9 or above and the other SAF forwarder is running EIGRP SAF rel8 or below.

Workaround: Make sure each SAF forwarder is running EIGRP rel8 or below, or rel9 or above.

- CSCtt26692

  Symptoms: The router crashes due to memory corruption. In the crashinfo, you may see:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk xxxxxxx data
  xxxxxxxx chunkmagic xxxxxxxx chunk_freemagic EF4321CD -
  Process= "CCSIP_SPI_CONTROL", ipl= 0, pid= 374
  chunk_diagnose, code = 1
  chunk name is MallocLite
  ```

  Conditions: This symptom is observed when the router is configured for SIP. When a translation-rule is configured to translate a number to one with more digits, the router may crash when the translation takes effect, such as when a call is forwarded.

  Workaround: Configuring “no memory lite” configurations can be used as a workaround in some cases (depending on the length of the phone numbers), but will cause the router to use more memory. If the translation-profile is configured to translate forwarded calls, then avoid or disable the option to forward the call.

- CSCtt34646

  Symptoms: IOMd crashes on the HA system.

  Conditions: This symptom occurs during normal reload, sometimes when standby shuts down completely and before coming up.

  Workaround: There is no workaround.

- CSCtu01601

  Symptoms: A Cisco ASR1000 series router may crash while executing the **write memory** command.

  Conditions: This issue may be triggered when the memory in the router is low.

  Workaround: There is no workaround.

- CSCtu36446

  Symptoms: The following error messages are displayed for the performance test with >20 CPS using the Cisco Radclient callsPerSecond Tool:

  ```
  Nov 10 12:56:32.953 EDT: %FMANRP_ESS-4-SESSCNT: ESS Provision Lterm Session:
  Unsupported peer_segtype= (0x15) Nov 10 12:56:32.955 EDT: %FMANRP_ESS-4-WRNPARAM_U:
  Get Lterm Peer ESS Segtype: Unsupported Peer SEGTYPE= (21) Nov 10 12:56:32.956 EDT:
  %FMANRP_ESS-4-WRNEVENT2: Ignoring Invalid ESS Segment: ESS segment/signature (0x0 /
  0x0) Nov 10 12:56:32.957 EDT: %SW_MGR-3-CM_ERROR_CLASS: Connection Manager Error:
  Class ADJ: - unable to unbind segment 2. Nov 10 12:56:32.958 EDT: %SW_MGR-3-CM_ERROR:
  Connection Manager Error - unprovision segment failed [ADJ:Lterm:43232] - hardware
  platform error.
  ```

  Conditions: This symptom is observed with high-scale, iEdge sessions.

  Workaround: There is no workaround.

- CSCtv36812

  Symptoms: An incorrect crashInfo file name is displayed during a crash.

  Conditions: This symptom is observed whenever a crash occurs.

  Workaround: There is no workaround.

- CSCtw53121

  Symptoms: ES+ goes into major state occasionally on reload or SSO.

  Conditions: This symptom is observed with the Cisco 7600 router with a 40 gig ES+ line card that is running Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCtw68089

  Symptoms: The routing event detector is not present on Integrated Services Routers such as the Cisco 2800 series.

  Conditions: This symptom occurs for all releases on generation one Cisco ISR routers running Cisco IOS Release 15.2(2)T.

  Workaround: There is no workaround.

- CSCtw70298

  Symptoms: A router crashes after the router boots up with scaled configuration and L2/L3 Distributed EtherChannel (DEC) or port-channel.

  Conditions: This symptom occurs only if there are more than two or more DFCs (ES+ and other equivalents) and with L2/L3 DEC configured such that one of the DFCs takes much longer to come up than the other.

  Workaround: There is no workaround.

- CSCtw98200

  Symptoms: Sessions do not come up while configuring RIP commands that affect the virtual-template interface.

  Conditions: This symptom is observed if a Cisco ASR1000 series router is configured as LNS.

  RIP is configured with the **timers basic** *5 20 20 25* command. Also, every interface matching the network statements is automatically configured using the **ip rip advertise** *5* command. These interfaces include the loopback and virtual-template interfaces too.

  On a Cisco ASR1000 series router, this configuration causes the creation of full VAIs which are not supported. Hence, the sessions do not come up. On Cisco ISR 7200 routers, VA subinterfaces can be created.

  Workaround: Unconfigure the **timers rip** command.

- CSCtx06813

  Symptoms: Installation fails, “rwid type l2ckt” error messages appear, and the VC may fail to come up on Quad-Sup router only. Though this error may appear for multiple other reasons, this bug is specific to Cisco Catalyst 6000 Quad-Sup SSO only.

  Conditions: This symptom is observed in a scaled scenario, doing second switchover on Quad-Sup router.

  Workaround: There is no workaround.

- CSCtx11598

  Symptoms: A router reload causes a Cisco Shared Port Adapter (SPA) failure with the following error message:

  ```
  % CWAN_SPA-3-FAILURE: SPA-2CHT3-CE-ATM[2/2]: SPA failure
  ```

  This failure can cause the SPA to go to one of the following states:

  – none

  - standby reset
  - down

  This failure leads to unexpected system reload.

  Conditions: This symptom is observed during router reload for 15-20 times.

  Workaround: Ensure that all of the library shared objects are loaded at the time of the SPA initialization.

- CSCtx23014

  Symptoms: HSRP hellos cannot be sourced from certain IPs.

  Conditions: This symptom is observed when HSRP hellos cannot be sourced for an IP address with a standby IP address in the same subnet and both are configured in the global VRF. For example:

```
Router(config)#interface Ethernet0/0
Router(config-if)# ip address 192.168.68.13 255.255.252.0
Router(config-if)# standby 68 ip 192.168.70.1
Router(config-if)# standby 68 priority 120
Router(config-if)# standby 68 preempt
Router(config-if)# arp timeout 300
```

  Workaround: Use an IP from the subnet for the SVI interface in the same VRF.

- CSCtx42751

  Symptoms: The following error message is displayed:

```
 %TRANSCEIVER-3-INIT_FAILURE: SIP2/0: Detected for transceiver module in
TenGigabitEthernet2/0/0, module disabled %LINK-3-UPDOWN: SIP2/0: Interface
 TenGigabitEthernet2/0/0, changed state to down
```

  Conditions: This symptom is observed with the XFP-10GLR-OC192SR transceiver.

  Workaround: Configure “service unsupported-transceiver”.

- CSCtx48753

  Symptoms: Higher memory usage with PPP sessions than seen in Cisco IOS XE Release 3.4/3.5.

  Conditions: This symptom is observed with configurations with PPP sessions. These will see up to 10% higher IOS memory usage than in previous images.

  Workaround: There is no workaround.

- CSCtx54882

  Symptoms: A Cisco router may crash due to Bus error crash at voip_rtp_is_media_service_pak .

  Conditions: This symptom has been observed on a Cisco router running Cisco IOS Release 15.1(4)M2

  Workaround: There is no known workaround.

- CSCtx66011

  A vulnerability in the Internet Key Exchange (IKE) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a device reload.

  The vulnerability is due to incorrect handling of malformed IKE packets by the affected software. An attacker could exploit this vulnerability by sending crafted IKE packets to a device configured with features that leverage IKE version 1 (IKEv1).

Although IKEv1 is automatically enabled on a Cisco IOS Software and Cisco IOS XE Software when IKEv1 or IKE version 2 (IKEv2) is configured, the vulnerability can be triggered only by sending a malformed IKEv1 packet.

In specific conditions, normal IKEv1 packets can also cause an affected release of Cisco IOS Software to leak memory.

Only IKEv1 is affected by this vulnerability.

An exploit could cause Cisco IOS Software not to release allocated memory, causing a memory leak. A sustained attack may result in a device reload.

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

This advisory is available at the following link:

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

Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

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

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

- CSCtx66030

  Symptoms: A Cisco router handling SIP registrations/unregistrations may unexpectedly reload. This symptom is observed on the following devices:

  - SIP-CME
  - SIP-SRST GW
  - CUBE

  Conditions: This symptom is observed when the number of SIP registrations/unregistrations handled is more than 320.

  Workaround: Limit the number of registrations/unregistrations to less than 320.

- CSCtx66046

  Symptoms: The Standby RP crashes with a traceback listing db_free_check.

  Conditions: This symptom occurs when OSPF NSR is configured. A tunnel is used and is unnumbered with the address coming from a loopback interface. A network statement includes the address of the loopback interface. This issue is seen when removing the address from the loopback interface.

  Workaround: Before removing the address, remove the network statement which covers he address of the loopback interface.

- CSCtx66804

  Symptoms: The configuration "ppp lcp delay 0" does not work and a router does not initiate CONFREQ.

  Conditions: This symptom is observed with the following conditions:

  - "ppp lcp delay 0" is configured.
  - The symptom can be seen on Cisco IOS Release 15.0(1)M5.

Workaround: Set delay timer without 0.

- CSCtx77501

  Symptoms: Traffic is dropped at the decap side of the PE box.

  Conditions: This symptom occurs with SSO at the decap side of an MVPN setup, DFC core-facing, 6748 access-facing.

  Workaround: Do a switchover.

- CSCtx79462

  Symptoms: OSPF neighborship does not get established.

  Conditions: This symptom is observed when enabling PFC on a multilink bundle in SIP-400. The OSPF neighborship does not get established.

  Workaround: There is no workaround. Disable PFC to bring up the OSPF neighborship.

  Further Problem Description: The OSPF hello packets get dropped by the peer end because the IP header is corrupted.

- CSCtx95840

  Symptoms: A Cisco voice gateway may unexpectedly reload.

  Conditions: This symptom is observed on a Cisco voice gateway running SIP protocol. In this case, the issue was when sipSPIUfreeOneCCB() returns, the leftover event is still being processed after CCB is released from sipSPIUfreeOneCCB(). Based on sipSPIStartRemoveTransTimer(ccb), CCB should have been released later by a background timer.

  Workaround: There is no workaround.

- CSCty01237

  Symptoms: The router logs show:

  ```
  <timestamp> %OER_BR-5-NOTICE: Prefix Learning STARTED
  CMD: 'show run' <timestamp>
  ```

  This is followed by the router crashing.

  Conditions: This symptom is observed under the following conditions:

  1. Configure PfR with a learn-list using a prefix-list as a filter and enable learn.
  2. Use a configuration tool, script or NMS that periodically executes **show run** on the MC over HTTP or some other means.

  Workaround 1: If you use the PfR learn-list feature, do not execute **show run** periodically.

  Workaround 2: If you use a monitoring tool that executes **show run** periodically, avoid using a learn-list configuration in PfR.

- CSCty03745

  Symptoms: BGP sends an update using the incorrect next-hop for the L2VPN VPLS address-family, when the IPv4 default route is used, or an IPv4 route to certain destination exists. Specifically, a route to 0.x.x.x exists. For this condition to occur, the next-hop of that default route or certain IGP/static route is used to send a BGP update for the L2VPN VPLS address-family.

  Conditions: This symptom occurs when the IPv4 default route exists, that is:

  ```
  ip route 0.0.0.0 0.0.0.0 <next-hop>.
  ```

  Or a certain static/IGP route exists: For example:

  ```
  ip route 0.0.253.0 255.255.255.0 <next-hop>.
  ```

Workaround 1: Configure next-hop-self for BGP neighbors under the L2VPN VPLS address-family. For example:

```
router bgp 65000
 address-family l2vpn vpls
  neighbor 10.10.10.10 next-hop-self
```

Workaround 2: Remove the default route or the static/IGP route from the IPv4 routing table.

- CSCty05092

  Symptoms: EIGRP advertises the connected route of an interface which is shut down.

  Conditions: This symptom is observed under the following conditions:

  1. Configure EIGRP on an interface.
  2. Configure an IP address with a supernet mask on the above interface.
  3. Shut the interface. You will find that EIGRP still advertises the connected route of the above interface which is shut down.

  Workaround 1: Remove and add INTERFACE VLAN xx.

  Workaround 2: Clear ip eigrp topology x.x.x.x/y.

- CSCty10285

  Symptoms: WCCP redirection does not happen with a Cisco ASR 1000 router running Cisco IOS XE Release 3.5 RP1.

  Conditions: This symptom occurs when GetVPN is used.

  Workaround: There is no workaround.

- CSCty22840

  Symptoms: A router can crash due to a Watchdog timeout on the NTP process as it fails to unpeer from an NTP peer that had already been removed. In addition, the following error might be seen in the system log:

  ```
  NTP Core (ERROR): peer struct for X.X.X.X not in association table
  ```

  Conditions: This symptom is observed when active changes occur in NTP, that is, new peers or servers are added at boot time as part of the existing configuration or during normal operation as part of a new configuration.

  Workaround: Configure NTP to use the ACL with the **ntp access-group peer** command to explicitly define which hosts can function as an NTP peer.

- CSCty24143

  Symptoms: The router does not pass IPv6 OSPF traffic.

  Conditions: This symptom occurs when the router passes traffic at the full line rate of a link.

  Workaround: Reduce the traffic rate by 10%.

- CSCty29230

  Symptoms: CMFIB entries are not being programmed on the SP and DFCs. Mroute shows both Accept and OILS, **ip mfib** output also shows Accept interface and Forwarding interface, but CMFIB entries are not programmed.

  Conditions: This symptom is observed with a Cisco 7600 router running a Cisco IOS Release 15.1(3)S throttle.

  Workaround: There is no workaround.

- CSCty38305

  Symptoms: The **xconnect vfi vpls** command gets rejected.

  Conditions: This symptom occurs while configuring “xconnect vfi vpls” under the interface VLAN. The error message “command rejected” is received.

  Workaround: There is no workaround.

- CSCty41336

  Symptoms: Forward-alarm ais does not work on CESoPSN circuits.

  Conditions: This symptom occurs when you create SAToP and CESoPSN circuits and configure “forward-alarm ais”.

  Workaround: There is no workaround.

- CSCty43587

  Symptoms: A crash is observed with memory corruption similar to the following:

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

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

  Workaround: There is no workaround.

- CSCty47231

  Symptoms: Traffic drops on removing the port-shaper.

  Conditions: This symptom is observed only when the policymap attach/detach is coupled with a link up/down. This issue is not seen on normal attach/detach. There are no issues with reload and policymap attached/detached.

  Workaround: Default the egress interface, and reconfigure; traffic recovers.

- CSCty51172

  Symptoms: The MAC address learned on L2 DEC on 7600-ES+40G3CXL is not installed as the primary entry on all the member interfaces, if the ingress traffic is on the nonhashed interface for that EFP.

  Conditions: This symptom occurs when Layer 2 distributed Etherchannel traffic is learned on a hashed interface first and then moved to a nonhashed interface.

  Workaround: Do not use Layer 2 distributed Etherchannel.

- CSCty53243

  Symptoms: Video call fails in the latest mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120303_065105_2.bin. This image has the uc_infra version: uc_infra@(mt_152_4)1.0.13. Note that video call works fine with the previous mcp_dev image asr1000rp2-adventerprisek9.BLD_MCP_DEV_LATEST_20120219_084446_2.bin.

  Conditions: This symptom is observed when CUBE changes the video port to “0” in 200 OK sent to the UAC.

  Workaround: There is no workaround.

- CSCty53923

  Symptoms: Broadcast traffic flows over the Standby Spoke VC and then gets punted.

Conditions: This symptom is observed when the nPE is the Cisco ME 3600X switch or the Cisco ME 3800X switch and the Standby Spoke VC terminates on it.

Workaround: There is no workaround.

- CSCty55449

  Symptoms: The device crashes after registering an Embedded Event Manager TCL policy.

  Conditions: If the policy uses the multiple event feature and the trigger portion is registered without curly braces (“{}”), then the device will crash. For example, this policy will trigger a crash:

```
::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger
::cisco::eem::correlate event 1 or event 2

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

action_syslog priority crit msg " triggered "
```

  Note how “::cisco::eem::trigger” is not followed by an opening curly brace.

  Workaround: Ensure that the trigger portion (that is, the correlate statement) is enclosed within curly braces. Given the example above, the proper syntax is:

```
::cisco::eem::event_register_syslog tag 1 pattern " pattern1"
::cisco::eem::event_register_syslog tag 2 pattern " pattern2"
::cisco::eem::trigger {
  ::cisco::eem::correlate event 1 or event 2
}

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

action_syslog priority crit msg " triggered "
```

- CSCty58992

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

  Conditions: This symptom is observed under the following conditions:

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

  Workaround: There is no workaround.

- CSCty64216

  Symptoms: On unconfiguring a scaled ACL, the router crashes.

  Conditions: This symptom is observed when an ACL having 1000 ACEs or more is unconfigured.

  Workaround: There is no workaround.

- CSCty66871

  Symptoms: The router stops forwarding traffic across one or more EoMPLS virtual circuits (VCs).
  Conditions: This symptom cccurs when you perform a shut/no shutdown on the MPLS TE tunnel carrying the VC.

  Workaround: Issue the clear xconnect command on the VC.

- CSCty68348

  Symptoms: If the OSPF v2 process is configured with the **nsr** command for OSPF nonstop routing, (seen after shutdown/no shutdown of the OSPF process), the neighbor is seen on standby RP as FULL/DROTHER, although the expected state is FULL/DR or FULL/BDR. As a result, after switchover, routes pointing to the FULL/DROTHER neighbor may not be installed into RIB.

  Conditions: This symptom is observed under the following conditions:

  – The OSPF router is configured for “nsr”.

  – Shutdown/no shutdown of the OSPF process.

  Workaround: Flapping of the neighbor will fix the issue.

- CSCty77582

  Symptoms: Traffic does not get classified in a DSCP-based class map for EVC in SW Eompls.

  Conditions: This symptom is observed when a policy map is applied to EVC in SW Eompls, and DSCP-based classification does not work.

  Workaround: There is no workaround.

- CSCty78435

  Symptoms: L3VPN prefixes that need to recurse to a GRE tunnel using an inbound route-map cannot be selectively recursed using route-map policies. All prefixes NH recurse to a GRE tunnel configured in an encapsulation profile.

  Conditions: This symptom occurs when an inbound route-map is used to recurse L3VPN NH to a GRE tunnel. Prefixes are received as part of the same update message and no other inbound policy change is done.

  Workaround: Configure additional inbound policy changes such as a community change and remove it prior to sending it out.

- CSCty79896

  Symptoms: Traffic drop is seen with 6rd tunnels having two ECMP paths to the core. Upon sending traffic with both ECMP paths (Gi4/14 and Gi4/5) active, traffic drops are seen as packets are software-switched and punted to RP. This issue is not seen with only one path active.

  The following steps summarize the issue:

  1. Both Gi4/14 and Gi4/5 should be unshut. Traffic flows through 4/14 but drops are seen.
  2. Frames are sent from Ixia - 4548658.

```
PE1#
PE1#sh interface counters | i 4/14
 Port        OutOctets        OutUcastPkts     OutMcastPkts    OutBcastPkts
Gi4/14      70829             999               6
 0
Gi4/14      19303273          229956          6
0           >>>>>>>>>>>. Only 229956 are sent out of 4548658

PE1#sh interface counters | i 4/5
Gi4/5       77143              1083           9                  0
Gi4/5       76176              1074           7                  0

PE1#sh int tu10 stat
Tunnel10
   Switching path    Pkts In    Chars In    Pkts Out    Chars Out
      Processor      0          0           0            0
    Route cache      0          0           228961       15111426
     >>>>>>>>>>>> Software switched
```

```
Distributed cache    0           0           0           0
       Total         0           0           228961      15111426
```

Conditions: This symptom is triggered when there are ECMP paths for the 6rd tunnels.

Workaround: You can recover by unconfiguring the ECMP paths and having a single path.

- CSCty86111

  Symptoms: The Cisco ISR G2 router crashes after “no ccm-manager fallback-mgcp” is configured.

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

  Workaround: There is no workaround.

- CSCty89224

  Symptoms: A Cisco IOS router may crash under certain circumstances when receiving an MVPNv6 update.

  Conditions: This symptom is observed when receiving an MVPNv6 update.

  Workaround: There is no workaround.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2012-3895 has been assigned to document this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

- CSCty96052

  Symptoms: A Cisco router may unexpectedly reload due to Bus error or SegV exception when the BGP scanner process runs. The BGP scanner process walks the BGP table to update any data structures and walks the routing table for route redistribution purposes.

  Conditions: This symptom is an extreme corner case/timing issue. This issue has been observed only once on a release image.

  Workaround: Disabling NHT will prevent the issue, but it is not recommended.

- CSCty96953

  Symptoms: The router drops traffic on an MLPPP bundle.

  Conditions: This symptom occurs after you perform a shutdown/no shutdown on an MLPPP bundle while the router is passing traffic.

  Workaround: Perform an OIR the interface module.

- CSCty99874

  Symptoms: Ingress policing is done on the EVC which does not have QoS policy.

  Conditions: This symptom is observed when one EVC has a QoS policy, and another does not. The QoS policy shows effect on the other EVC also.

  Workaround: Attach a dummy policy to the other EVC. Or attach and detach a policy on the other EVC.

- CSCtz00430

  Symptoms: The static route is removed from the routing table.

  Conditions: This symptom is observed when pulling out and replacing a connection to the management interface.

Workaround 1: Default the management interface and reconfigure IP.

Workaround 2: Do a shut and no shut on the management interface through the CLI.

- CSCtz03559

  Symptoms: MVPN is seen on the Cisco ME 3600X and ME 3800X switches.

  Conditions: This symptom is observed as currently, there are two SDM templates present in the Cisco ME 3600X and ME 3800X switches. Both templates do not support MVPN. A new SDM template is needed on the license “AdvancedMetroIPAccess” to support the MVPN.

  Workaround: MVPN cannot be used without the new SDM template.

- CSCtz06611

  Symptoms: IPsec tunnel states are UP-IDLE because of broadcast packets that are punted to the CPU. The mac-address of VPN-SPA is not learned properly.

  Conditions: This symptom is a timing issue. You may see it the first time or need to try multiple times. This symptom is seen with the crypto map plus vrf configuration.

  1. Reload the router with above configuration: the mac-address changes to all FF.
  2. Default the configuration of VLAN (where crypto map and engine is applied), then configure it again with old configuration. Now the mac-address will show all FF. 3. Create the vlan. Do a **no shutdown**. Attach vrf. Then add crypto map to it.

  Workarounds: For the steps mentioned in condition section above, below are the workarounds respectively.

  Workaround 1: Remove and add “ip vrf forwarding” and then remove and add the **crypto engine** command.

  Workaround 2: Remove and add the **crypto engine** command. Workaround 3: Do a **shut/no shut** on the VLAN interface.

- CSCtz08719

  Symptoms: With split horizon, traffic does not flow on all BDs.

  Conditions: This symptom is observed when traffic does not flow on all BDs.

  Workaround: There is no workaround.

- CSCtz08746

  Symptoms: On the 12in1 Serial SPA with hardware version lower than 2.0, an upgrade using “test upgrade” with the latest Cisco 7600 FPD bundles results in the SPA FPD device being downgraded from version 1.2 to 1.1. Subsequently, both auto and manual upgrades fail to bring the SPA FPD version back to 1.2. The SPA goes to the OutOfServ or FpdUpReqd state.

  Conditions: This symptom is observed only with the older SPA hardware (hardware version lower than 2.0) when it is plugged into a SIP200 or SIP400 on the Cisco 7600 platform.

  Workaround: Use the latest SPA hardware (hardware version 2.0 or above).

- CSCtz11876

  Symptoms: The **show ethernet cfm maintenance-points local** command output shows type BD and ID 0 after MTU is changed on the interface that has a service instance with xconnect. This issue is also seen if the backup peer is changed under xconnect.

  Conditions: This symptom is observed when Ethernet CFM MEP is configured on an xconnect service instance.

  Workaround: Remove MEP and reapply.

- CSCtz12525

  Symptoms: Accounting stop is sent without Acct-Input-Packets Acct-Output-Packets Acct-Input-Octets Acct-Output-Octets when service stop is performed.

  Conditions: This symptom is observed when service stop is issued for the prepaid service.

  Workaround: There is no workaround.

- CSCtz13465

  Symptoms: High CPU is seen on Enhanced FlexWAN module due to interrupts with traffic.

  Conditions: This symptom is observed with an interface with a policy installed.

  Workaround: There is no workaround.

- CSCtz13818

  Symptoms: In a rare situation when route-map (export-map) is updated, IOS is not sending refreshed updates to the peer.

  Conditions: This symptom is observed when route-map (export-map) is configured under VRF and the route-map is updated with a new route-target. Then the IOS does not send refreshed updates with modified route-targets.

  Workaround 1: Refresh the updated route-target to use **clear ip route vrf** *vrf-name net mask*.

  Workaround 2: Hard clear the BGP session with the peer.

- CSCtz24047

  Symptoms: Free process memory is being depleted slowly on linecards in the presence of the DLFIoATM feature configured on a PA-A6-OC3 (enhanced Flexwan). Finally memory allocation failures are observed. Use the show memory proc stat history command to display the history of free process memory.

  Conditions: This symptom occurs when Slow Proc Memory depletion is observed on 7600-ES+ cards when installed on a Cisco 7600 router that has DLFIoATM configured on a PA-A6-OC3 hosted on an enhanced Flexwan module.

  Workaround: There is no workaround.

- CSCtz25953

  Symptoms: The “LFD CORRUPT PKT” error message is dumped and certain length packets are getting dropped.

  Conditions: This symptom is observed with a one-hop TE tunnel on a TE headend. IP packets with 256 or multiples of 512 byte length are getting dropped with the above error message.

  Workaround: There is no workaround.

- CSCtz26188

  Symptoms: Packet loss is observed on platforms in certain deployments having a large number of prefixes routing traffic onto a TE tunnel.

  Conditions: This symptom occurs if the configured value of the cleanup timer is 60 seconds, then packets might be lost on the platforms where the forwarding updates take longer.

  Workaround: Configure the value of the cleanup timer to 300 seconds.

  ```
  mpls traffic-eng reoptimize timers delay cleanup 300
  ```

- CSCtz26658

  Symptoms: The Cisco ASR 1000 router acts as GET VPN GM. Small UDP fragments (21 to 25 bytes, IP header included) coming in through IPsec are dropped.

  Conditions: This symptom occurs when the Cisco ASR 1000 router acts as GET VPN GM and TBAR is enabled for the group.

  Workaround: There is no workaround. Disabling TBAR is not recommended as a workaround due to the operational impact of the change on a live GET VPN network.

- CSCtz30983

  Symptoms: Crash on ES+ line card upon issuing the **show hw-module slot X tech- support** or **show platform hardware version** command. This is similar to CSCti78408 but not to CSCti78408.

  Conditions: This symptom occurs on an ES+ line card.

  Workaround: Do not issue the **show hw-module slot X tech- support** or **show platform hardware version** command on an ES line card unless explicitly mentioned by Cisco.

- CSCtz35061

  Symptoms: Flexlink switchover causes VLAN to not be allowed in trunk link.

  Conditions: This symptom is related to flexlink switchover caused by instantaneous link flapping.

  Workaround: There is no workaround.

- CSCtz37863

  Symptoms: IPCP is not in an open state and it does not seem to be calling the This-Layer-Down (TLD) vector.

  Conditions: This symptom is observed if IPv4 saving is enabled and IPCP negotiation failed because of a TermReq received from peer.

  Workaround: There is no workaround.

- CSCtz38558

  Symptoms: The following traceback may be seen on a Cisco ASR 1000 router when processing some IPv6 packets:

```
Apr 18 17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
TS:00000176080579214858 %INFRA-3-INVALID_GPM_ACCESS: Invalid GPM Load at 800268cd HAL
start 3fc0 HAL end 413f INFRA start 409e INFRA 4140 NET 340d0
-Traceback=1#002b3a75f6cabf53c25612ed4553871e 804b0d63 804b1204
8046c212 80020708 800268cd 80026cd0 80435955 806509bb
Apr 18 17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
TS:00000176080579433103 %INFRA-3-INVALID_GPM_ACCESS_INFO: 80026cd0
0002fdb0 0002fdd4 0002fdd0 00000002 00000001 00000001 0003413f
00000001 00000000 00000000 00001000 93b9bac0 8ba80000 fffffffd 00201000 Apr 18
17:20:27.554: %IOSXE-3-PLATFORM: F1: cpp_cp: QFP:0.0 Thread:132
TS:00000176080579587035 %INFRA-3-INVALID_GPM_ACCESS_DATA: e188f4a8aa3ef3a0
 205e84e72c9f6761 4486ffd3c38d7e12 b0c71bf4a146b4ba 8e786f7e673d2e56
9308160a565df75c 952e4a0fe2ef327c 1cff673d2be0f8bf
48248a1e150a1ce9 e1386aed768ad28c e6d23cd54b68619e c49866ce95863bf6
c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a
c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a c99d8c7d5a2e4a8a
c99d8c7d5a2e4a8a 8553c53af0e4f16e
```

  Conditions: This symptom occurs when the IPv6 packet is malformed.

  Workaround: There is no workaround.

  Additional Information: The packet will be dropped.

- CSCtz41048

  Symptoms: The **trace mpls ipv4** command is unsuccessful.

  Conditions: This symptom is observed with the **trace mpls ipv4** command.

  Workaround: There is no workaround.

- CSCtz46300

  Symptoms: Traffic is not classified under the QoS ACLs having port matching using range (inclusive range), lt (less than), and gt (greater than) operators.

  Conditions: This symptom is seen with IPv4 and IPv6 with L4 port ranger operations using range, lt, and gt, which do not work with QoS ACLs on Cisco ME 3600 and Cisco ME3800 switches.

  Workaround: There is no workaround.

- CSCtz46399

  Symptoms: VLAN RAM is not programmed with the correct VPN number for a few VRFs.

```
Eagle2-es20-dfc4#sh mls vlan-ram 1182
1182 TYCHO Vlan RAM
Key: * => Set, - => Clear

vlan    nf-vpn mpls mc-base siteid stats rpf vpn-num bgp-grp l2-metro
rpf-pbr-ovr
-------+-----+-------+-----+-----------+------+-----+---+-----------+----------+------
----+-----------
1182    -       -       *      0        0       -       -     0           0
        -          *
```

  Conditions: This symptom is observed with the OIR of the ES-20 line card with scaled MVPNv6 configuration and 50 VRFs configured.

  Workaround: There is no workaround.

- CSCtz47309

  Symptoms: When using smart defaults in FlexVPN, the mode transport may be sent from initiator even if “tunnel” is configured.

  Conditions: This symptom was first seen on a Cisco ASR router running Cisco IOS Release 15.2(2)S and a Cisco ISR router running Cisco IOS Release 15.2(3)T. It is seen with FlexVPN.

  Workaround: Use smart defaults on both sides on of the tunnel.

- CSCtz52844

  Symptoms: Excessive memory is being held by SG DPM process.

  Conditions: This symptom has been observed on a Cisco 10000 router running Cisco IOS Release 12.2(33)SB10 when some users send many duplicate DHCP discover messages.

  Workaround: Clear the sessions intermittently.

- CSCtz59041

  Symptoms: After router reload, the agent succeeds but with the following errors:

```
*Apr 26 11:22:42.455 IST: %DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping
database Read succeeded.
*Apr 26 11:22:42.455 IST: %DHCP_SNOOPING-6-VLAN_NOT_SUPPORTED: Vlan not supported. 150
bindings ignored
```

Conditions: This symptom occurs when some LCs such as ES+ take more time to come up compared to others. If there are SVIs on these on which snooping is enabled, some bindings might get dropped after router reload.

Workaround: Force a retry using the **renew** command.

- CSCtz61153

  Symptoms: The Cisco ASR 903 router does not establish BFD neighbors over port-channel 16.

  Conditions: This symptom occurs when you configure BFD on port-channel 16 between two Cisco ASR 903 routers.

  Workaround: Configure BFD on port-channels 1-15.

- CSCtz61274

  Symptoms: BFD sessions remain DOWN post peer node reload.

  Conditions: This symptom occurs when BFD RX gets impacted post reload of the peer node as it fails to do a proper lookup on the GAL label. This issue is seen intermittently.

  Workaround: There is no workaround.

- CSCtz62680

  Symptoms: “DFC WAN Line Card Software Element Not Found - QOS: TCAM Class ID” errors appear along with BADCHUNKFREEMAGIC errors, leading to an ES20 crash.

  Conditions: This symptom occurs when service policies less than 128 kb are added or removed.

  Workaround: There is no workaround.

- CSCtz63974

  Symptoms: Mcast T/F forwarding fails for some EVCs with Trunk EFP’s Encapsulation change.

  Conditions: This symptom is observed under the following conditions:

  1. Configure Trunk EVCs with the range of allowed VLANS.
  2. Initiate Mcast traffic to allowed BDIs.
  3. While Multicast data traffic is on, change the Encapsulation definition to add/delete few VLANs and check the replication.

  Workaround: There is no workaround.

- CSCtz66284

  Symptoms: IOMD crash may be seen.

  Conditions: This symptom is observed when bringing up the interfaces on an HA system.

  Workaround: There is no workaround.

- CSCtz66770

  Symptoms: When under ATM PVC (SPA-4XOC3-ATM or v2) with MUX encapsulation and OAM enabled, L3 policy-map is applied and PVC goes down.

  Conditions: This symptom occurs when policy-map sets DSCP (to 7) for default- class, and it affects OAM communication.

  Workaround: Use aal5snap encapsulation.

- CSCtz67785

  Symptoms: The Cisco ASR 1000 router may experience a CPP crash.

Conditions: This symptom occurs when the router is configured for Session Border Controller (SBC). During periods of high traffic, FP reports a lot of media up events to RP, which can crash FP.

Workaround: If "ip nbar protocol-discovery" is enabled, it may exacerbate the crashes. Removing it may help provide some stability.

- CSCtz71940

  Symptoms: The Present Active crashes on issuing the SSO CLI.

  Conditions: This symptom occurs when performing switchover on the HA system.

  Workaround: There is no workaround. The Present Active (new standby) comes up fine again even after it crashes. There is no functionality impact.

- CSCtz72390

  Symptoms: The name mangling functionality is broken. Authorization fails with the "IKEv2:AAA group author request failed" debug message.

  Conditions: This symptom is observed with Cisco IOS Release 15.2(3)T.

  Workaround: There is no workaround.

- CSCtz72615

  Symptoms: All interfaces on a Cisco 7600-SIP-200 are down after Cisco IOS downgrade.

  Conditions: This symptom is observed on Cisco 7600 series routers.

  Workaround: There is no workaround.

- CSCtz73836

  Symptoms: The router crashes.

  Conditions: This symptom is observed when the router is running NHRP.

  Workaround: There is no workaround.

- CSCtz74229

  Symptoms: The rate at which ARP requests are triggered by traffic being sent to a destination in which the ARP is not resolved is very low.

  Conditions: This symptom occurs when traffic is being sent to multiple destinations in which the ARP is not resolved.

  Workaround: There is no workaround.

- CSCtz74685

  Symptoms: A router crash is observed on Y1731 DM.

  Conditions: This symptom is seen when starting 1DM session.

  Workaround: There is no workaround.

- CSCtz75641

  Symptoms: The router drops traffic over a port-channel.

  Conditions: This symptom occurs when you perform the following sequence of events:

  - Configure and bundle gi0/0/0 into a port-channel.
  - Remove gi0/0/0 from port-channel.
  - Another link (it may be gi0/0/0 if it is added back or any other interface) bundles to the port-channel

  Workaround: Reload the router.

- CSCtz77171

  Symptoms: Subscriber drops are not reported in mod4 accounting.

  Conditions: This symptom is observed on checking policy-map interface for account QoS statistics on a port-channel subinterface.

  Workaround: There is no workaround.

- CSCtz78194

  Symptoms: A Cisco ASR 1000 that is running Cisco IOS XE Release 3.6 or Cisco IOS Release 15.2(2)S crashes when negotiating multi-SA DVTI in an IPsec key engine process.

  Conditions: This symptom is observed with the Cisco ASR configured to receive DVTI multi-SA in aggressive mode and hitting an ISAKMP profile of a length above 31.

  Workaround: Shorten the ISAKMP profile name to less than 31.

- CSCtz79488

  Symptoms: Multicast replication fails for some of the EFPs post removal/recreation of BDIs.

  Conditions: This symptom is observed under the following conditions:

  1. There are 255 EVCs on a single port, attached to 255 BDIS (1:1).
  2. Configure the policy map on each EVC.
  3. Initiate Multicast data traffic to a single Multicast group.
  4. Remove some of the BDIS and recreate with Multicast data traffic on. Replication fails post recreation of BDIS.

  Workaround: Perform shut/no shut on the 255 EVCs configured interface.

- CSCtz80643

  Symptoms: A PPPoE client's host address is installed in the LNS's VRF routing table with the **ip vrf receive** *vrf name* command supplied either via RADIUS or in a Virtual-Template, but is not installed by CEF as attached. It is instead installed by CEF as receive, which is incorrect.

  Conditions: This symptom is observed only when the Virtual-access interface is configured with the **ip vrf receive** *vrf name* command via the Virtual-Template or RADIUS profile.

  Workaround: There is no workaround.

- CSCtz82232

  Symptoms: The following error message is displayed:

  IOSXE_INFRA-6-PROCPATH_CLIENT_HOG: on reload, traffic fails post Reload

  Conditions: This symptom is observed under the following conditions:

  - Multicast data traffic to a single Multicast group with 255 OIFs. - 255 EVCs on single port with a policy map on each EVC. - All 255 BDIS send IGMPv3 SSM joins to a single Multicast group. - Reload the box and observe the Hog messages.

  Workaround: There is no workaround.

- CSCtz82265

  Symptoms: IOSd crash is seen on the Cisco ASR 903 router while reloading all IMs continuously on the setup.

  Conditions: This symptom is observed with MPLS-TP configurations and 510 BFD sessions.

  Workaround: There is no workaround.

- CSCtz82711

  Symptoms: Datapath session would

  Conditions: This symptom is observed when SGSN sends echo req before PDP_CREATE_REQ.

  Workaround: There is no workaround.

- CSCtz85907

  Symptoms: A Cisco 7600 should have an MVPNv4 configuration and the system replication mode as egress. Now, if “address-family ipv6” is configured under the VRF definition, MVPN traffic might be affected.

  Conditions: SREx and RLSx releases.

  Workaround: Use ingress replication.

- CSCtz86024

  Symptoms: There is a long delay in joining mcast stream with Cisco IOS 15S releases that are running on RP.

  Conditions: This symptom is observed when there is no (*,G) on the box, and the first packet for the stream creates this entry.

  Workaround: With static joins we can make sure that entry is present in mroute table.

- CSCtz86763

  Symptoms: Sessions remain partially created, and memory is consumed and not returned.

  Conditions: This symptom occurs when sessions are churned and reset before they reach active state.

  Workaround: There is no workaround.

- CSCtz89485

  Symptoms: NAT traffic passes through the new standby router following HSRP switchover.

  Conditions: This symptom is observed with HA NAT (NAT with HSRP) mappings with inside global addresses that overlap a subnet owned by a router interface.

  Workaround:

  1. Force a HSRP switchover so that the initial standby router takes activity.
  2. Remove and readd HSRP NAT mappings on the newly active router.
  3. Force a HSRP swtichover back to the initial active router.

- CSCtz90154

  Symptoms: Rapid getVPN re-registration by GM when IPsec failure occurs during initial registration. Multiple ISAKMP SAs created and deleted per second.

  Conditions: This symptom is observed on a Cisco ASR 1000 router that is running Cisco IOS Release 15.2(1)S or Cisco IOS Release 15.2(1)S2 as a GM.

  Workaround: There is no workaround.

- CSCtz93922

  Symptoms: An xconnect virtual circuit may be down on one peer while it is up on the remote peer. The output of the **show mpls l2 transport vc detailed** command indicates that it is in the LruRrd state and that the last status it received from the remote peer is pw-tx-fault.

  Conditions: This symptom has been observed when both the attachment circuit and core-facing interfaces are on the same module and that module is reset using the **hw-module module** *module* **reset** command, and the remote peer is running Cisco IOS Release 15.2(02)S or later releases.

Workaround: Do s**hutdown** followed by **no shutdown** on the attachment circuit.

- CSCtz95745

  Symptoms: BGP PIC core is broken on shutting an ECMP path towards the BGP next-hop. When one ECMP path is shut, traffic drop is seen for 4-5 seconds and full traffic is recovered after some time.

  Conditions: This symptom occurs when there are uneven number of paths towards two or more BGP next-hops and one path is shut.

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

- CSCtz97755

  Symptoms: ES card crash and alignment tracebacks on SP are seen.

  Conditions: This symptom is observed with IPv6 unicast and multicast traffic up and running. Unconfiguring IPv6 unicast-routing will lead to this issue.

  Workaround: There is no workaround.

- CSCtz99916

  Symptoms: The Cisco 3945 router does not respond to a reinvite from CVP.

  Conditions: This symptom occurs when call legs are not handled in a proper IWF container.

  Workaround: There is no workaround.

- CSCua04085

  Symptoms: Port-channel member links show as UP when port-channel is admin down.

  Conditions: This symptom is only a display issue.

  Workaround: There is no workaround.

- CSCua07228

  Symptoms: Locally generated traffic is not encrypted when crypto map is applied to the LISP interface.

  Conditions: This symptom occurs when GET VPN or static crypto map is configured on the LISP interface to encrypt traffic between LISP E-IDs.

  Workaround: There is no workaround.

- CSCua08027

  Symptoms: Tracebacks appear on a Cisco ASR router when LI is used with SNMP-based TAP. This issue is seen with Cisco IOS XE Release 3.5S.

  Conditions: This symptom occurs when SNMP-based LI is used with routers running Cisco IOS XE Release 3.5S or later releases.

  Workaround: There is no workaround.

- CSCua08471

  Symptoms: Traffic may go to a wrong destination post switchover on the Cisco ASR 903 router.

  Conditions: This symptom is observed with the VPLS over MPLS-TP scenario. This is an extremely rare scenario, and is seen in less than once out of 50 attempts. The hardware entry corresponding to the VC/TP label is wrongly programmed.

  Workaround: Reconfigure the affected VC post switchover.

- CSCua10377

  Symptoms: A Cisco router with Circuit Emulation SPA may suffer an SPA crash.

  Conditions: This symptom occurs when the CE T1 circuit is configured by the end user for AT&T FDL, and the end user transmits FDL messages requesting 4- hour or 24-hour performance statistics.

  Workaround: There is no workaround. If possible, contact the end user and have them reconfigure their device for ANSI FDL.

- CSCua13418

  Symptoms: RP-Announce packets are being replicated across all the tunnel interfaces and the count of replication is equal to the number of tunnel interfaces. For example, if there are 3 tunnel interfaces, then each tunnel should forward 1 RP-Announce packet each minute (with the default timer configured). However, in this case, each tunnel is forwarding 3 RP-Announce packets across each tunnel interface. This issue is not specific to the number of interfaces. It can happen with any number of tunnel interfaces.

  Conditions: This symptom is observed when filter-autorp is configured with the **ip multicast boundary** command. This issue is seen on the Cisco 3725 router too, where the incoming packets are being replicated because of the **filter-autorp** command.

  Workaround: Removing filter-autorp resolves the issue. However, you need to remove the **pim** and **boundary** commands first and then reapply the pim and boundary list without the **filter-autorp** keyword. Also, doing this might lead to redesigning of the topology to meet specific requirements.

  ```
  int Tun X no ip pim sparse-dense mode no ip multicast boundary XXXXXX filter-autorp
  int TuX ip pim sparse-dense mode ip multicast boundary XXXXXX
  ```

- CSCua16046

  Symptoms: Some packets are dropped when multiple streams are merging on the Cisco ME3600X and ME3800X switches. Sometimes, packet drops are seen with a single stream as well.

  Conditions: This symptom is observed with smaller size packets such as 64-512 bytes.

  Workaround: The workaround depends on the release. With some release, “no ip igmp snooping” will resolve the issue.

- CSCua16786

  Symptoms: When a Cisco 7600 router is placed as a mid-hop-router between the first hop router (FHR) and rendezvous point (RP), with P2P GRE tunnel interface as the FHR facing interface, then PIM-registration might not get completed. The unicast PIM-registration packet might get dropped at the Cisco 7600 router.

  Conditions: This symptom is seen in Cisco IOS Release 12.2(33)SRE6 and RLSx releases.

  Workaround: Delete and create the FHR facing p2p tunnel interface at Cisco 7600 router, which is acting as mid-hop-rtr.

- CSCua18051

  Symptoms: The Cisco ASR 903 router sends duplicated Multicast packets with RPF changes.

  Conditions: This symptom is observed under the following conditions:

  1. Initially, no costs are configured.
  2. Configure OSPF cost to the link to change the RPF path.
  3. Post RPF change, the Cisco ASR 903 router egresses duplicated packets.

  Workaround: There is no workaround.

- CSCua19425

  Symptoms: RP crashes at the far end, pointing to Watchdog Process BGP.

  Conditions: This symptom is observed when doing an FP reload at the near end. This issue is seen with EBGP sessions with BFD configured between near end and far end routers.

  Workaround: There is no workaround.

- CSCua22599

  Symptoms: MCB timeout error message is seen on console. Ports 7 and 8 do not come up.

  Conditions: This symptom is seen when combo ports come up with media-type.

  Workaround: There is no workaround.

- CSCua22755

  Symptoms: The ACL missed blocked ARP reply packets. As a result, the I/F could not learn ARP.

  Conditions: This symptom is observed when the port has 254 BDI I/F, and those 254 BDI I/F have the same ACL. Some of the VLANs ACL blocked ARP reply.

  Workaround: There is no workaround.

- CSCua23997

  Symptoms: Continuous ESP crash is seen after dropping packets due to unsupported OCE.

  Conditions: This symptom is observed when OCE is unsupported.

  Workaround: There is no workaround.

- CSCua25671

  Symptoms: After adding the source interface in RSPAN, there is huge flooding to all trunks allowing RSPAN VLAN starts, even if there is no traffic on the RSPAN source interface.

  Conditions: This symptom is observed under the following conditions:

  1. The router has a RSPAN source session.
  2. The source interface being added to the RSPAN source session is on ES+.
  3. Any of the ES+ modules in the system has an interface on the RSPAN VLAN (that is, at least one of the interfaces on an ES+ module carries RSPAN replicated traffic).
  4. The online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, are enabled on the ES+ module which has 2 and 3 mentioned above.

  Workaround 1: Disable the online diagnostic tests, TestFabricCh0Health and TestFabricCh1Health, on the ES+ module which has the RSPAN source.

  Workaround 2: If you have to use an interface on the ES+ module as a SPAN source, make sure that no other interface on any of the ES+ modules in the system is in the RSPAN VLAN. If you have to use an interface on the ES+ module to carry RSPAN replicated traffic, make sure that no other interface on any of the ES+ modules in the system is being monitored as an RSPAN source.

- CSCua25748

  Symptoms: The PW receive counter does not work.

  Conditions: This symptom is observed only with the ES+ card. This issue is not seen always due to timing events.

  Workaround: Flap VC again, and check if the counter works. If it does not work, reconfigure the VC.

- CSCua26487

  Symptoms: SNMP loops at OID 1.3.6.1.4.1.9.9.645.1.2.1.1.1, and as a result, SNMP walk fails.

  Conditions: This symptom is observed only on the SNMP getbulk request on 1.3.6.1.4.1.9.9.645.1.2.1.1.1.

  Workaround: Exclude the MIB table from SNMP walk using SNMP view. See the below configurations.

```
snmp-server view <view name> iso included
snmp-server view <view name> ceeSubInterfaceTable excluded
snmp-server community <community> view <view name>nterfaceTable excluded
snmp-server community <community> view <view name>
```

- CSCua27842

  Symptoms: The Cisco ASR 1000 router crashes in Firewall code due to NULL l4_info pointer. Day 1 issue.

  Conditions: This symptom occurs when the Cisco ASR 1000 router acts as the MPLS L3VPN UHP. It crashes because FW/NAT requires the l4_info to be set. To trigger this issue, the following features must be configured:

  1. MPLS L3VPN (PE).
  2. Zone-Based FW/NAT.
  3. MPLS & MP-BGP loadbalance configured towards the upstream router.

  Workaround: There is no workaround.

- CSCua30259

  Symptoms: EVC egress traffic does not flow. The frames are dropped by Selene.

  Conditions: This symptom occurs when SPAN is configured on service instance.

  Workaround: There is no workaround.

- CSCua31794

  Symptoms: After reload with the debug image, framed E1 lines are down.

  Conditions: This symptom occurs when checking “show controller SONET”. The default controller framing mode is taken as “crc4”. However, before reload, the configuration for those E1s were configured as “no-crc4”. When configured on the E1s as “no-crc4”, it works fine, and the “show controller SONET” framing output changes to “no-crc4”. As per the running configuration, the configuration does not “no-crc4”, as the default is CRC4. When configuring “no-crc4”, it does not show in the running configuration and is not saved. After reload, it again shows CRC4 and services go down again.

  Workaround: Configure E1s as “no-crc4” and they will work fine, but such changes are not being saved in the configuration. If reload reoccurs, all these services go down again.

- CSCua33287

  Symptoms: ES+: L2TPv3 entries are programmed incorrectly after restart.

  Conditions: This symptom is observed when some L2TPv3 sessions are established on ES+ module. After the restart of ES+, some np entries may not program correctly. As the result, ES+ will stop to transmit packets.

  This condition will recover after executing **shut/no shut** on physical interfaces.

  Workaround: There is no workaround.

- CSCua33527

  Symptoms: Traceback seen after second or third switchover:

  ```
  %LFD-SW2-3-SMBADEVENT: Unexpected event CO_WAIT_TIMEOUT for state RUNNING -Traceback=
  7908E9Cz 7909848z 79099CCz 7909B9Cz 78DBF20z 523292Cz 522C1D4z
  ```

  Conditions: This symptom is observed with a quad-sup scenario/setup. This traceback is seen on the new active RP after second switchover onwards.

  Workaround: There is no workaround.

- CSCua34638

  Symptoms: A crash is seen on RP2, when the **show platform software shell command package** command is issued.

  Conditions: This symptom is observed when the **show platform software shell command package** command is issued. It impacts the RP2 (x86_64_*) image only.

  Workaround: There is no workaround. Do not issue the **show platform software shell command package** command.

- CSCua39107

  Symptoms: In a FlexVPN Spoke to Spoke setup, Resolution reply goes via the Tunnel interface to the Hub.

  Conditions: This symptom is only observed when NHO is added for the V-Access, overriding an existing route. This issue is not seen when H route is added.

  Workaround: Distribute the summarized address from the Hub, thus avoiding addition of NHO at the Spokes. The Spokes will then add H route instead of NHO.

- CSCua40790

  Symptoms: Memory leaks when SNMP polling cbgpPeer2Entry MIB.

  Conditions: This symptom occurs when BGPv4 neighbors are configured.

  Workaround: There is no workaround if this MIB is to be polled.

- CSCua42089

  Symptoms: Configuring Ingress redirection for service group 61 (Mask) and applying an extended ACL in the outbound direction on the same interface causes software switching even when there are no punt entries in the TCAM.

  Conditions: This symptom is observed when WCCP service 61 with Mask assignment in the Ingress indirection, along with an outbound ACL, is configured on the same interface.

  Workaround: Do not configure the outbound ACL along with a WCCP service.

- CSCua43930

  Symptoms: Checksum value parsed from GRE header is not populating causing the GRE tunnel checksum test case to fail.

  Conditions: This symptom is observed on a Cisco ISR G2.

  Workaround: There is no workaround.

- CSCua48584

  Symptoms: The Cisco ME 3600X's ARP resolution may fail after flexlink switchover.

  Conditions: This symptom is observed on the Cisco ME 3600X running Cisco IOS Release 15.2(S) or Cisco IOS Release 15.2(2)S1 with flexlink configured.

Workaround: Shut the active port of the flexlink pair. In other words, do a manual switchover through CLI.

- CSCua62054

  Symptoms: Egress DSCP classification does not work when a policy is applied on the main interface which has trunk EFP configured.

  Conditions: This symptom is observed when a DSCP-based service policy is configured on the main interface and it does not classify the traffic for DSCP.

  Workaround: Use normal EFP instead of trunk.

- CSCua62102

  Symptoms: Traffic is classified based on prec/dscp/tos, along with Layer 4 (TCP/UDP) ACLs in the service policy. This issue is not seen without ACLs.

  Conditions: This symptom is observed when you configure policy-map matching prep/dscp/tos with Layer 4 TCP/UDP ACLs in the ingress direction.

  Workaround: There is no workaround.

- CSCua64546

  Symptoms: In a scaled setup with IPV4 and IPV6 ACL together (not necessarily on the same interface), IPV4 ACLs may stop working if the IPV6 ACL configured later overwrites the IPv4 ACL results and vice versa.

  Conditions: This symptom is observed with IPV4 and IPV6 ACLs configured on the box.

  Workaround: There is no perfect workaround. Reconfiguring the IPV4 ACL can recover the functionality but will affect the IPV6 ACL.

  Further Problem Description: Only the IPV4 or IPV6 ACL configuration will work.

- CSCua64700

  Symptoms: The IPsec tunnel state goes to Up-Idle after 4-5 days of the router being up and running.

  Conditions: This symptom is observed if you have low rekey value, as with the rekey, the new SPI gets allocated. This issue is seen with WS-IPSEC-3 and to verify this, check the below counter.

  ```
  show crypto ace spi
  ```

  If there is no decrement in the SPI allocated counter and there is a consistent increment in the counter, the chances are high that you will encounter this issue.

  Once the value reaches 61439, you will encounter this issue.

  ```
  MTCVPNK03#sh cry ace spi
  SPI in use ........................... 0
  Normal SPI allocated ................. 61439
  ```

  Workaround: There is no workaround. You need to reload the box.

- CSCua68398

  Symptoms: The ES+ card crashes.

  Conditions: This symptom is observed with a scaled EVC and VPLS configurations.

  Workaround: Stop the traffic. After the line cards boot up and the ports are up, start the traffic.

- CSCua79516

  Symptoms: SYN packets to establish ftp-data connections are sporadically dropped at the Cisco ASR router.

Conditions: This symptom is observed under the following conditions:

- Using the active mode FTP.
- Using PAT.
- The symptom is observed on a Cisco ASR 1000 router.

Workaround 1: Use the passive mode FTP.

Workaround 2: Use the static NAT/dynamic NAT configuration.

- CSCua85837

  Symptoms: Depending on the aces in the redirect-list ACL used, only a subnet of the traffic gets redirected based on ports.

  Conditions: This symptom is observed when the WCCP service has a redirect-list ACL applied which in turn has port-specific aces in them.

  Workaround: Remove the L4 operators from the redirect-list ACL.

- CSCua85934

  Symptoms: A session provisioning failure is seen in the ISG-SCE interface. The deactivate or disconnect request has the message authenticator wrongly calculated.

  Conditions: This symptom is observed with the ISG-SCE interface.

  Workaround: There is no workaround.

- CSCua87877

  Symptoms: A crash occurs in ucode.

  Conditions: This symptom is observed with 160cps SIP calls.

  Workaround: There is no workaround.

- CSCua98690

  Symptoms: The ES+/ES20/SIP-400 (any card which supports EVC) card may crash due to memory corruption.

  Conditions: This symptom is observed when the MAC ACL is configured on EFP.

  Workaround: There is no workaround.

- CSCub01576

  Symptoms: ESP reloads on the Cisco ASR 1000 router due to ucode crash.

  Conditions: This symptom is observed on the Cisco ASR 1000 router where the Layer 4 Redirect feature is configured. This problem was first introduced in Cisco Release 15.2(01)S. This issue may be not seen at all in some customer environments to about once a week in medium-sized high CPS ISG production networks.

  Workaround: There is no workaround.

- CSCua09073

  Symptoms: If 6708 generates txCRC errors, CSCtq73026 accounts for these errors in TestErrorMonitor diagostic test and takes the necessary recovery action. But for CSCtq73026 to be invoked, the TestErrorMonitor test should be included in the test suite for 6708. This test is missing and hence, the fix in CSCtq73026 will also not be invoked.

  Conditions: See the description of CSCtq73026. For this fix to be take effect, TestErrorMonitor should be added in the test suite. In this DDTS, we are adding this test so that in case of an error, as mentioned in CSCtq73026, recovery action will be triggered.

Workaround: There is no workaround.

- CSCtq48455

  Symptoms: After Flex Link failover, all VLAN SVIs associated with VLANs forwarding on the Flex Link interfaces go down.

  Conditions: This symptom is observed with Flex Links configured with VLAN SVIs.

  Workaround: Remove the Flex Links and then reconfigure them.

- CSCtw51052

  Symptoms: HSRP hello packets are dropped on a Cisco ME 3600X switch when there are two Cisco ME 3600X switches acting as switches between the HSRP boxes, and there is a port-channel connecting the two ME 3600 switches with both the Tengig ports as its members. HSRP is configured on VLANs.

  Conditions: This symptom is not seen consistently. It is seen only on a few VLANs while the others may be working as expected.

  Workaround: Removing and readding the VLANs fixes the issue. Issue the **no vlan** *vlan-id* command followed by the **vlan** *vlan-id* command. Removing and adding the VLAN from the port-channel and its members may also fix the issue.

- CSCtx54990

  Symptoms: The **static mac address** command disappears randomly on reload on a Cisco ME 3600X switch running the me360x-universalk9-mz.151-2.EY image.

  Conditions: This symptom occurs randomly. This issue has been seen in several customer switches and in the lab.

  Workaround: Reapply the **static** commands after reload. There is no other workaround.

- CSCty20330

  Symptoms: SNMP requests a large block of memory.

  ```
  Feb 15 23:44:28.285 CST: %SYS-2-MALLOCFAIL: Memory allocation of 2424504504
  bytes failed from 0x15047BC, alignment 0
  Pool: Processor  Free: 803990516  Cause: Not enough free memory
  Alternate Pool: None  Free: 0  Cause: No Alternate pool
   -Process= "SNMP ENGINE", ipl= 0, pid= 264
  ```

  Conditions: This symptom is observed with SNMP.

  Workaround: There is no workaround.

- CSCtz48867

  Symptoms: In the customer network, this problem was triggered under the following situation:

  ```
  Active WG          Standby WG

     |                  |

     |                  |

  Active BR -------- Standby BR

     |

     |

  Client
  ```

"Active BR" and "Standby BR" are two Cisco ME 3600X switches. The link between the two Cisco ME 3600X switches is an etherchannel (two member ports). Multicast traffic from the "Active WG" and "Standby WG" flow down the path. The multicast clients join the multicast group via an SVI interface in the two switches and the L2 etherchannel between the switches trunks that particular VLAN.

In a normal situation, the client should be able to receive multicast streams 224.0.1.x (from Active WG) and 224.0.127.x (from Standby WG). After Active BR is reloaded, multicast streams 224.0.127.x can no longer be forwarded from the Standby BR to the Active BR.

Conditions: This symptom occurs when the Active BR is reloaded. In a normal situation, the client should be able to receive multicast streams 224.0.1.x (from Active WG) and 224.0.127.x (from Standby WG). After the Active BR is reloaded, multicast streams 224.0.127.x can no longer be forwarded from the Standby BR to the Active BR.

Workaround: After a "clear ip mroute *" in the standby BR, the problem is resolved.

- CSCua84606

  Symptoms: With L2PT tunnel or forwarding, the Cisco ME 3600X switch or the Cisco ME 3800X switch cannot process more than two VLAN tags. Such packets get dropped.

  Conditions: This symptom is observed with L2PT tunnel or forwarding. The Cisco ME 3600X switch or the Cisco ME 3800X switch cannot process more than two VLAN tags. Such packets get dropped.

  Workaround: There is no workaround.

- CSCtw79171

  Symptoms: Platform asserts at adjmgr_l2_create.

  Conditions: This symptom occurs with excessive flapping of a link.

  Workaround: There is no workaround.

- CSCty50421

  Symptoms: With control word set (C bit) explicitly in MPLS bindings for the VC, the L2PT tunnel over EFP xconnect does not work.

  Conditions: This symptom is observed when control word is set (C bit) explicitly in MPLS bindings for the VC.

  Workaround: Disable control word.

- CSCua14594

  Symptoms: Memory leak is seen when polling for the following PW MIBS:

```
1.3.6.1.4.1.9.10.106.1.5.1.1 (cpwVcPerfTotalInHCPackets)
1.3.6.1.4.1.9.10.106.1.5.1.2 (cpwVcPerfTotalInHCBytes)
1.3.6.1.4.1.9.10.106.1.5.1.3 (cpwVcPerfTotalOutHCPackets)
1.3.6.1.4.1.9.10.106.1.5.1.4 (cpwVcPerfTotalOutHCBytes)

Address    Size   Alloc_pc  PID  Alloc-Proc       Name
34417B84      308 13774B30  473  SNMP ENGINE     AToM VC event trace
```

  This memory leak, on repeated polling, may lead to device crash.

  Conditions: This symptom is observed with Cisco IOS Release 3.6S upon polling of the SNMP VC statistics query.

  Workaround: There is no workaround.

- CSCub25360

Symptoms: In a Flexlink switchover scenario, it seems that for some reason, the Cisco ME 3600X switch does not sent out a dummy Mcast packet for the SVI.

Conditions: This symptom is observed with a Cisco ME 3600X Flexlink switchover.

Workaround: There is no workaround.

- CSCtg47129

  Symptoms: Enhancements in NAT processing are seen in VRF environments.

  Conditions: This symptom is observed with packets that need NAT in a VRF.

  Workaround: There is no workaround.

- CSCua66308

  Symptoms: Classification-related error messages and tracebacks are seen on the CLI console, and the configuration is not downloaded to the data path.

  Conditions: This symptom is observed with large configurations with multiple deny statements.

  Workaround: Observe caution when using deny statements in a configuration.

- CSCuc68092

  Symptoms: A CPU hog and an LDP flap is seen on executing the **sh int transceiver detail** command.

  Conditions: This symptom occurs after executing the **sh int transceiver detail** command for the first time after the box is reloaded.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(2)S1

Cisco IOS Release 15.2(2)S1 is a rebuild release for Cisco IOS Release 15.2(2)S. The caveats in this section are resolved in Cisco IOS Release 15.2(2)S1 but may be open in previous Cisco IOS releases.

- CSCtl01184

  Symptoms: Sometimes an EVC that is configured on ES+ sends frames out with CFI bit set in the VLAN tag.

  Conditions: This symptom is observed on EVCs that are configured on ES+.

  Workaround: There is no workaround.

- 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.

- 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.

- 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

- CSCtt99627

  Symptoms: The **lacp rate** and **lacp port priority** commands may disappear following a switchover from active to standby RP.

  Conditions: This affects the Cisco 7600 platform.

  Before performing a switchover one may check the configuration on the standby RP to see if the commands are present or not. If the commands are not present on the standby RP then they will disappear if a switchover occurs.

  Workaround: Prior to switchover if the commands do not show up on the standby RP as described above, then unconfiguring and reconfiguring the command on the active RP will fix the issue.

  Otherwise if the commands disappear after a switchover then the commands must be reconfigured on the newly active RP.

- CSCtu32301

  Symptoms: Memory leak may be seen.

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

  Workaround: Do not run the show commands frequently.

- CSCtu35052

  Symptoms: Sweep ping fails when an ATM interface is configured with AAL5 encapsulation.

  Conditions: This symptom occurs when the ATM packet size is greater than 1484 bytes.

  Workaround: There is no workaround.

- CSCtu40028

  Symptoms: The SCHED process crashes.

  Conditions: The issue occurs after initiating TFTP copy.

Workaround: There is no workaround.

- CSCtw46061

  Symptoms: The following output shows the leaked SA object continuing to be in the "OBJECT_IN_USE" state. The state is supposed to be changed to OBJECT_FREEING by crypto_engine_delete_ipsec_sa(). This is in turn being called by ident_free_outbound_sa_list().

```
shmcp-fp40#sh crypto eli
Hardware Encryption : ACTIVE
Number of hardware crypto engines = 1
CryptoEngine IOSXE-ESP(14) details: state = Active
Capability    : DES, 3DES, AES, RSA, IPv6, GDOI, FAILCLOSE

IKE-Session   :     0 active, 12287 max, 0 failed
DH            :   211 active, 12287 max, 0 failed
IPSec-Session :   323 active, 32766 max, 0 failed
```

  Conditions: This symptom is observed on a Cisco ASR 1000 series router

  Workaround: There is no workaround.

- 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.

- CSCtw80678

  Symptoms: Multilink PPP ping fails when the serial interfaces experience QMOVESTUCK error.

  Conditions: This symptom may be observed if multilink PPP member links and serial interfaces on which the QMOVESTUCK error is reported are on the same SPA.

  Workaround: There is no workaround.

- CSCtw95466

  Symptoms: When a large number of Ethernet or VLAN xconnect sessions are configured on a Cisco 7600 router, the Supervisor Processor may reload.

  Conditions: This symptom is observed when **aaa new-model** is configured.

  Workaround: Configure **no aaa new-model**.

- 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.

- CSCtw99991

  Symptoms: Chunk memory leak is seen in the ES+ LC after configuring the IP source guard EVC configurations.

Conditions: This issue is seen on a Cisco 7600 router with ES+ LC running Cisco IOS interim Release 15.2(01.16)S.

Workaround: There is no workaround.

- CSCtx02522

  Symptoms: The router displays intermittent traceback errors.

  Conditions: Occurs when you configure REP.

  Workaround: There is no workaround.

- CSCtx04709

  Symptoms: Some EIGRP routes may not be removed from the routing table after a route is lost. The route is seen as “active” in the EIGRP topology table, and the active timer is “never”.

  Conditions: This symptom is seen when a multiple route goes down at the same time, and query arrives from neighbor router. Finally, neighbor detects SIA for affected router and neighbor state is flap. However, active entry is remaining after that, and route is not updated.

  Workaround: The **clear ip eigrp topology** *network mask* command may remove unexpected active entry.

- CSCtx11740

  Symptoms: The traffic convergence takes longer because of additional/unwanted traffic is punted to CPU as we do not have *,GM code changes. The *,GM entries help drop the traffic that is not needed by MFIB (PI) code.

  Conditions: This symptom is seen with link and node failures in dual-home scenarios.

  Workaround: There is no workaround.

- CSCtx32329

  Symptoms: When using the **show ipv6 rpf** command, the router crashes or displays garbage for RPF idb/nbr.

  Conditions: This symptom can happen when the RPF lookup terminates with a static multicast route that cannot be resolved.

  Workaround: Do not use static multicast routes, or make sure that the next hop specified can always be resolved. Do not use the **show** command.

- CSCtx35064

  Symptoms: Traffic remains on blackholed path until holddown timer expires for PfR monitored traffic class. Unreachables are seen on path, but no reroute occurs until holddown expires.

  Conditions: This symptom is seen under the following conditions:

  – MC reroutes traffic-class out a particular path (BR/external interface) due to OOP condition on the primary path.

  – Shortly after enforcement occurs, an impairment on the new primary path occurs causing blackhole.

  – PfR MC does not declare OOP on the new primary path and attempt to find a new path until holddown timer expires. Causes traffic loss.

  Workaround: Reduce the holddown timer to 90 seconds (minimum value) to minimize impact.

- CSCtx37768

  Symptoms: QoS classification does not match traffic against an egress policy map between MPLS and IP access.

Conditions: This symptom is observed when a QoS policy is applied on an EVC bridge domain interface.

Workaround: Use one of the following workarounds:

- Reload the router.
- Remove and re-apply an encapsulation configuration such a VLAN.
- Remove and re-attach the bridge domain under the EVC.
- Perform a **shutdown/no shutdown** on the BDI interface.

- 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 Cisco IOS core dump.

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

- CSCtx66011

  A vulnerability in the Internet Key Exchange (IKE) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a device reload.

  The vulnerability is due to incorrect handling of malformed IKE packets by the affected software. An attacker could exploit this vulnerability by sending crafted IKE packets to a device configured with features that leverage IKE version 1 (IKEv1).

  Although IKEv1 is automatically enabled on a Cisco IOS Software and Cisco IOS XE Software when IKEv1 or IKE version 2 (IKEv2) is configured, the vulnerability can be triggered only by sending a malformed IKEv1 packet.

  In specific conditions, normal IKEv1 packets can also cause an affected release of Cisco IOS Software to leak memory.

  Only IKEv1 is affected by this vulnerability.

  An exploit could cause Cisco IOS Software not to release allocated memory, causing a memory leak. A sustained attack may result in a device reload.

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

  This advisory is available at the following link:

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

  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

- CSCtx80078

  Symptoms: Packets are getting punted to CPU or being forwarded with EVC mac security.

  Conditions: This symptom is seen with implicit deny of packets with routable IPv4 header.

Workaround: There is no workaround.

- CSCtx82775

  Symptoms: Calls on the Cisco ASR 1000 series router seem to be hung for days.

  Conditions: The symptom is observed when MTP is invoked for calls.

  Workaround: Reload the router or perform a no sccp/sccp.

- CSCtx84948

  Symptoms: A Cisco ASR 1000 series router malfunctions after consecutive ESP crashes triggered by CSCtr56576. This symptom is observed when the interfaces are up/up but are not sending traffic. You can also identify this state using the following command:

  ```
  Router#show platform software interface fp active name GigabitEthernet5/0/0
  Name: GigabitEthernet5/0/0, ID: 23, QFP ID: 22, Schedules: 4096
  Type: PORT, State: disabled, SNMP ID: 16, MTU: 1500   <<<<<<
  ```

  The output of the command indicates that at the ESP level, the interface is disabled and can not forward traffic.

  Conditions: The Cisco ASR 1000 series router has redundant ESPs and consecutive ESP crashes. This symptom has been caused only by CSCtr56576.

  Workaround: **Shut/no shut** the disabled interface to resume the traffic.

- CSCtx85247

  Symptoms: An ES20 line card is reset on doing redundancy switchover of RSPs.

  Conditions: This symptom is seen with redundancy switchover of RSPs.

  Workaround: There is no workaround.

- CSCtx85489

  Symptoms: A memory leak is followed by a router crash.

  Conditions: This issue is seen in a Cisco 7600 router that is running Cisco IOS Release 15.2(2)S. Configuring and unconfiguring PBR “N” number of times from an interface triggers the crash. The root cause for this issue is that each time when PBR is configured and unconfigured, memory is leaked.

  Workaround: There is no workaround.

- CSCtx91831

  Symptoms: IP address of the SVI interface is not installed in the routing table.

  Conditions: When we have an IP address configured for the BD, the following sequence of configurations puts the box in a state where the corresponding ip- address is not installed in the routing table.

  ```
  no vlan <vlan-id> --- same as the BD
  Int vlan <vlan-id> shutdown --- At this point the Int vlan goes down no shutdown
  vlan <vlan-id>
  ```

  This issue seen only when we have SVI and BD EFP and will not be seen for SVI and trunk ports.

  Workaround: A **shut/no shut** of the interface VLAN after adding the **vlan** *vlan-id* command fixes the problem.

- CSCtx94279

  Symptoms: A line card crashes.

Conditions: This symptom is observed in switch traffic and flood traffic (line rate and less that 128-byte packet size) with more than one port in the egress path flood.

Workaround: There is no workaround.

- CSCtx94393

  Symptoms: ESP crashes at fman_avl_free.

  Conditions: The symptom is observed with the following conditions:

  - Scale IKEv2 4k IPsec sessions with FlexVPN dVTI server.
  - Scale IKEv1 1k IPsec sessions with dVTI server.
  - CAC (50) enabled on both server and clients.
  - DPD (60/15/on-demand) enabled.
  - Do a **clear crypto session** per 20 minutes on server.
  - 20M bidirectional traffic

  Workaround: There is no workaround.

- CSCtx94772

  Symptoms: Cannot configure xconnect on an SVI when an RFP having the same BD is configured with pop 2 symmetric.

  Conditions: This issue is seen only when EFP is configured first and then the xconnect over SVI.

  Workaround: Configure the xconnect over SVI before configuring the RFP with the same pop 2 and same BD.

- 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 line card.

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

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

- CSCty14596

  Symptoms:

  1. PIM neighbor is not established over routed pseudowire.
  2. PW cannot pass PIM traffic when destination LTL in DBUS header is 0x7ff8.

  Conditions: These symptoms are seen under the following conditions:

  - Configure PIM over routed pseudowire.
  - Core facing card is ES+.
  - Outgoing interface of the PW is a TE Tunnel over the physical interface.
  - Cisco IOS 15.0(1)S and later releases.

  Workaround: Make the outgoing interface of PW:

  1. Over physical interface only (i.e. without tunnel).
  2. TEFRR over port-channel interface.
  3. Issue will not be observed on ES20.
  4. Issue will not be observed in Cisco IOS Release 15.0(1)S and later releases.

- CSCty16620

  Symptoms: Backup pseudowire in SVIEoMPLS does not come up after reloading the router.

  Conditions: This symptom is seen under the following conditions:

  1. Remote PE on the backup PW does not support pseudowire status TLV.
  2. The “no status TLV” is not configured in pw-class used in the PW, which does not support pseudowire status TLV.

  Workarounds:

  Proactive workaround: Configure “no status TLV” into the pw-class used if the remote side does not support status TLV.

  Reactive workaround: Reprovision the backup pseudowire after reload.

- CSCty19713

  Symptoms: The ESP or CPP of a Cisco ASR 1000 series router crashes.

  Conditions: This symptom is observed in the NAT Application Layer Gateway (ALG) for DNS packets.

  Workaround: There is no workaround.

- CSCty23747

  Symptoms: MAC address withdrawal messages are not being sent.

  Conditions: This symptom is seen with flapping REP ports on UPE.

  Workaround: There is no workaround.

- CSCty28384

  Symptoms: The police actions are not accepted if given in different commands.

  Conditions: If police actions are given in different commands, they are not accepted.

  Workaround: Configure the policer actions in a single command.

- CSCty28796

  Symptoms: The **show snmp mib | in flash** command on the router does not show any flash entries. Also snmpwalk for flash objects shows the following error:

  ```
  "No Such Object available on this agent"
  ```

  Conditions: This symptom is observed on Cisco ME 3600X and ME 3800X.

  Workaround: There is no workaround.

- CSCty30886

  Symptoms: A standby RP reloads.

  Conditions: This symptom is observed when bringing up PPPoE sessions with configured invalid local IP address pool under virtual-template profile and “aaa authorization network default group radius” on the box with no radius present. No IP address is assigned to PPPoE Client.

  Workaround: There is no workaround.

- CSCty32728

  Symptoms: CPU hog is seen when MVPN configuration is replaced with another using the **configure replace** command.

  Conditions: This symptom is observed on a stable MVPN network when replacing the configuration with dual-home receiver/source configuration once the router comes up with the tunnel.

Workaround: There is no workaround.

- CSCty34200

  Symptoms: In MVPN scale environment, a crash is observed after “no ip multicast-routing”. A memory leak is observed after changing data MDT address.

  Conditions: This symptom is seen in MVPN scale scenario.

  Workaround: There is no workaround.

- CSCty42626

  Symptoms: Certificate enrollment fails for the Cisco 3945 router and the Cisco 3945E router due to digital signature failure.

  Conditions: This symptom is observed when the Cisco 3945 router or the Cisco 3945E router enrolls and requests certificates from a CA server.

  Workaround: There is no workaround.

- CSCty45999

  Symptoms: The “aps group acr 1” line disappears after power off and on a Cisco 7600 router in working and protection groups.

  Conditions: This symptom occurs when the Cisco 7600 router suddenly loses power, and the “aps group acr 1” line does not appear again. If you run the **show controller SONET 1/1/0** command, you will see every E1 on “unconfigured” status.

  Workaround: Delete the “aps protect 1 X.X.X.X” & “aps working 1” lines. The “framing” must be changed in order to delete every E1 channel configuration, then “framing” should be configured as it was in the beginning. Then “aps group acr 1” line is configured as well as “aps protect 1 X.X.X.X” and “aps working 1” lines. Finally every E1 must be configured as it was before this issue occurs. You can copy the E1 configuration before to delete anything and then paste it at the end.

- CSCty46022

  Symptoms: A Cisco ASR 1000 experiences high ESP CPU constantly.

  Conditions: The symptom is observed when ISG sessions with DHCP initiator are experiencing fragmented traffic and the fragmented traffic has a small packet size. The packets will be punted to ESP CPU and cause it to be busy.

  Workaround: There is no workaround.

- CSCty51088

  Symptoms: On a Cisco ME 3600X or Cisco ME 3800X, when traffic for a group (S2,G) is sent to an interface that is already acting as the source for another group (S1,G), it does not receive any traffic since no (S2,G) entry is formed.

  Conditions: This symptom is observed when the receiver interface is already a source interface for another multicast stream.

  Workaround: None

- CSCty52047

  Symptoms: IKE SAs are not getting deleted by DPD (crypto isakmp keepalive).

  Conditions: This symptom is observed on a Cisco ASR 1000 router with DPD enabled.

  Workaround: Manually delete the stuck isakmp session:

  clear crypto isakmp conn-id

  You can get the conn-id from the output of the **show crypto isakmp sa** command.

- CSCty54319

  Symptoms: OSPF and protocols using 224.0.0.x will not work btw CE-CE over a VLAN.

  Conditions: This symptom occurs when IGMP snooping is disabled.

  Workaround: Toggle IGMP snooping two times.

- CSCty54885

  Symptoms: The Standby RP crashes when the Active RP is removed to do a failover.

  Conditions: This symptom is observed when the last switchover happens with redundancy forced-switchover.

  Workaround: Do a switchover only with redundancy forced-switchover instead of removing the RP physically.

- CSCty57746

  Symptoms: On the Cisco ASR 903 router, the **show environment** command displays incorrect values, including P0 and P1 voltages and Amps values.

  Conditions: This symptom is observed with the Cisco ASR 903 router when you apply the **show environment** command.

  Workaround: There is no workaround.

- 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.

- CSCty61212

  Symptoms: The removal of crypto map hangs the router.

  Conditions: This symptom is observed with the removal of GDOI crypto map from interface.

Workaround: There is no workaround.

- CSCty62559

  Symptoms: On the Cisco ASR 1000 series router, FP crash occurs at cpp_qm_obj_add_to_parent with 8k xconnects.

  Conditions: This symptom is observed with the Cisco ASR 1000 series router while doing SPA reload after RP switchover with 8k xconnects.

  Workaround: There is no workaround.

- CSCty62887

  Symptoms: When more than 1024 DTL requests are made during free sip msg_info pool, the Cisco ASR 1000 will crash.

  Conditions: Multiple factors could contribute to this. It depends on the number of messages contained in SIP ALG.

  Workaround: There is no workaround.

- CSCty68402

  Symptoms: NTT model 4 configurations are not taking effect.

  Conditions: This symptom occurs under the following conditions:

```
policy-map sub-interface-account
 class prec1
  police cir 4000000 conform-action transmit  exceed-action drop
  account
 class prec2
  police cir 3500000 conform-action transmit  exceed-action drop
  account
 class prec3
  account
  class class-default fragment prec4
  bandwidth remaining ratio 1
  account

policy-map main-interface
 class prec1
  priority level 1
  queue-limit 86 packets
 class prec2
  priority level 2
  queue-limit 78 packets
 class prec3
  bandwidth remaining ratio 1
  random-detect
  queue-limit 70 packets
  class prec4 service-fragment prec4
  shape average 200000
  bandwidth remaining ratio 1
  queue-limit 62 packets
```

```
 class class-default
  queue-limit 80 packets
```

Workaround: There is no workaround.

- CSCty76106

  Symptoms: Crash is seen after two days of soaking with traffic.

  Conditions: This symptom occurs with node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, constant frequent polling of SNMP, RCMD, full scale of routes and bidirectional traffic.

  Workaround: There is no workaround.

- CSCty81700

  Symptoms: When a remote PE reloads in MVPN network, it causes a memory leak.

  Conditions: This symptom occurs when core interface flap or remote PE node reloads causing a small amount of memory leak. If the node stays up experiencing a lot of core interface/remote PE outages, it can run out of memory and fail to establish PIM neighborship with remote PEs.

  Workaround: There is no workaround. As a proactive measure, user can periodically (depending on n/w outages) run the **show memory debug leak chunk** command and reload the node, if there are a lot of memory leaks reported by this command.

- CSCty82888

  Symptoms: Removing an ATM Permanent Virtual Path (PVP) by the **no atm pvp** command while it is configured with the **xconnect** command causes a memory leak. This can be observed using the **show circuit memory** command:

```
Router#show acircuit memory | include AC ctx chunks
  AC ctx chunks              :        200/32820      (  0%) [      2] Chunk
```

  Also, on a dual-RP system with stateful switchover enabled, if the PVP is immediately reconfigured and the **xconnect** command is added, the standby RP may reload.

  Conditions: These symptoms have been observed on Cisco routers that are running Cisco IOS Release 15.2(2)S.

  Workaround: Unconfigure the xconnect using the **no connect** command before removing the PVP.

- CSCty91955

  Symptoms: L2-switched traffic loss within a BridgeDomain routed traffic via an SVI experiences no loss.

  Conditions: This symptom occurs with BridgeDomain that has both tagged and untagged EVCs. Issue should not happen with like-to-like scenario.

  Workaround: Make sure there is like-to-like (tagged-to-tagged or untagged-to- untagged) communication.

- CSCty93290

  Symptoms: Momentary traffic loss of multicast traffic with QoS configuration on EFP is observed.

  Conditions: This symptom is seen under the following conditions:

  1. Have multiple VLANs in OIF list.
  2. Each VLAN should have only one EFP/sp.
  3. Have QoS configured on EFPs.

  Workaround: There is no workaround.

- CSCty96049

  Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. An attacker could exploit this vulnerability by sending a single DHCP packet to or through an affected device, causing the device to reload.

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

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

- CSCty96263

  Symptoms: Under periods of transient interface congestion, an MPLS-TP network may experience unnecessary traffic switchovers or longer than expected restoration times.

  Conditions: This symptom is observed during periods of transient interface congestion. Behavior will be caused by loss of pseudowire status packets. Lack of a classification mechanism for these packets prevents user from protecting them with a QoS policy.

  Workaround: There is no workaround.

- CSCty96579

  Symptoms: Under periods of transient interface congestion, an MPLS-TP network may experience unnecessary traffic switchovers or longer than expected restoration times.

  Conditions: This symptom is observed during periods of transient interface congestion. Behavior will be caused by loss of vital OAM packets (e.g. AIS/LDI, LKR). Lack of a classification mechanism for these packets prevents from protecting them with a QoS policy.

  Workaround: There is no workaround.

- CSCty99331

  Symptoms: CPU hog messages are seen on the console.

  Conditions: This symptom is seen when applying huge rmap with more than 6k sequences on an interface.

  Workaround: There is no workaround.

- CSCty99711

  Symptoms: SIP-400 crash may be observed due to illegal memory access.

  Conditions: This symptom is observed with Cisco IOS Release 12.2(33)SRE4 when SIP-400 has PPPoE session scale.

  Workaround: There is no workaround.

- CSCtz01361

  Symptoms: Traffic gets black holed when TE auto-backup is enabled on midpoint router and FFR is configured on the P2MP TE tunnel head end.

  Conditions: This symptom is seen when enabling FRR on the head end with auto- backup already configured on the box.

  Workaround: Remove auto-backup configuration from the midpoint router.

- CSCtz04090

  Symptoms: In a VRRP/HSRP setup, traffic from particular hosts is getting dropped. Ping from the host to any device through the VRRP routers fails.

  Conditions: This symptom is usually seen after a VRRP/HSRP switchover. The packet drops because of some packet loop that is created between the routers running VRRP/HSRP.

Workaround: A clear of the MAC table on the new VRRP master usually restores the setup to working conditions.

- CSCtz13451

  Symptoms: A Cisco ME 3800X and Cisco ME 3600X switch may experience CPU HOG errors and then a watchdog crash or memory corruption.

  Conditions: This symptom is observed when running many of the **show platform mpls handle** commands. The switch may crash.

```
SW#sh platform mpls handle 262836664 ?
  BD_HANDLE              bd/el3idc_vlan handle
  L2VPN_L2_HANDLE        l2 tunnel intf handle
  L2VPN_PW_BIND_DATA     pw bind data
  LFIB_TABLE             LFIB TABLE handle
  PORT_HANDLE            port/met handle
  RW_HANDLE              Rewrite handle
  SW_OBJ_ADJACENCY       oce type SW_OBJ_ADJACENCY
  SW_OBJ_ATOM_DISP       oce type SW_OBJ_ATOM_DISP
  SW_OBJ_ATOM_IMP        oce type SW_OBJ_ATOM_IMP
  SW_OBJ_DEAGGREGATE     oce type SW_OBJ_DEAGGREGATE
  SW_OBJ_EGRESS_LABEL    oce type SW_OBJ_LABEL
  SW_OBJ_EOS_CHOICE      oce type SW_OBJ_EOS_CHOICE
  SW_OBJ_FIB_ENTRY       oce type SW_OBJ_FIB_ENTRY
  SW_OBJ_FRR             oce type SW_OBJ_FRR
  SW_OBJ_GLOBAL_INFO     oce type SW_OBJ_GLOBAL_INFO
  SW_OBJ_ILLEGAL         oce type SW_OBJ_ILLEGAL
  SW_OBJ_IPV4_FIB_TABLE  oce type SW_OBJ_IPV4_FIB_TABLE
  SW_OBJ_IPV6_FIB_TABLE  oce type SW_OBJ_IPV6_FIB_TABLE
  SW_OBJ_LABEL_ENTRY     oce type SW_OBJ_LABEL_ENTRY
  SW_OBJ_LABEL_TABLE     oce type SW_OBJ_LABEL_TABLE
  SW_OBJ_LOADBALANCE     oce type SW_OBJ_LOADBALANCE
  SW_OBJ_RECEIVE         oce type SW_OBJ_RECEIVE
```

  Workaround: Do not run the commands as they are for development use.

- CSCtz16622

  Symptoms: A Cisco ME 3600X acts as a label disposition Edge-LSR when receiving MPLS packets with Checksum 0xFFFF that will continue to drop with Ipv4HeaderErr and Ipv4ChecksumError at nile.

  Conditions: This symptom is seen with label pop action at the Edge-LSR.

  Workaround: There is no workaround.

- CSCtz27782

  Symptoms: A crash is observed on defaulting service instance with OFM on EVC BD configured.

  Conditions: This symptom occurs when interface is in OAM RLB slave mode.

  Workaround: There is no workaround.

- CSCtz31888

  Symptoms: After state change of one of the L3 uplink interfaces, STP cost of BPDU PW increases from 200 to 2M, which can lead to blocking state in STP for this PW.

  Conditions: This symptom occurs with state change of one of the uplink L3 interfaces.

  Workaround: Increase the cost of access ring to more then 2M to avoid blocking of the BPDU PW.

- CSCtz32521

  Symptoms: In interop scenarios between Cisco CPT and Cisco ASR 9000 platforms, in order to support transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Conditions: This symptom occurs in interop scenarios between Cisco CPT and Cisco ASR 9000 platform. In order to support transport switchover requirement for 50 msec, it would require Cisco ASR 9000 or PI code to allow configuration or negotiation of minimal interval timer to 2.

  Workaround: There is no workaround.

- CSCtz35467

  Symptoms: QoS policy-map gets detached from interface on line protocol down-- >up transition happens on reload, admin **shut/no shut** and interface flap as well.

  Conditions: This symptom is observed when QoS policy-map is applied at interface and more than one child has “priority + police cir percent x” configured.

  Workaround: To be preventive use “police cir *absolute”* instead of “police cir percent x”. To be reactive use EEM applet/script.

  Further Problem Description: There is no error message in the syslog, only on console. It seems that line protocol UP can be used as the trigger action for EEM.

- CSCtz40435

  Symptoms: The L4 port-range security ACL does not work on EVC.

  Conditions: This symptom is seen when security ACL containing L4 port range operation that is applied on EVC. The behavior is not as expected. The same works on physical interface.

  Workaround: Add support for L4 port range operation similar to the case of applying it on physical interface.

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

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

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

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

- CSCtz45057

  Symptoms: High CPU is observed on the Cisco ME 3800X.

  Conditions: This symptom occurs with a loop of OTNIFMIB that causes CPU Hog and crash on Cisco ME 3800X during pulling from PPM

  Workaround: OTNIFMIB is not supported or required on Cisco ME 3800X and Cisco ME 3600X. Disable them while pulling from PPM.

- CSCtz46300

  Symptoms: Traffic is not classified under the QoS ACLs having port matching using range (inclusive range), lt (less than), and gt (greater than) operators.

  Conditions: This symptom is seen with IPv4 and IPv6 with L4 port ranger operations using range, lt, and gt, which do not work with QoS ACLs on Cisco ME 3600 and Cisco ME 3800 switches.

  Workaround: There is no workaround.

- CSCtz54823

  Symptoms: Configuration is getting locked on chopper SPA.

  Conditions: This symptom happens as follows:

  1. Shut down the controller of the SPA.
  2. Reload will bring the SPA in the locked state.

  Workaround: There is no workaround. Erase start up and reload the system to get back to configuration mode.

Open Caveats—Cisco IOS Release 15.2(2)S

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

- CSCts81627

  Symptoms: On Cisco IOS Release 15.1(2)EY1a, REP Flaps when BFD is configured on the same device. On Cisco IOS Release XE 3.6.0S, REP with fast hellos flaps when BFD is configured on the same device.

  Conditions: This symptom occurs when REP and BFD sessions with aggressive timers are configured on the same device. We could have REP flaps.

  Workaround: On Cisco IOS Release 15.1(2)EY1a, there is no workaround if both REP and BFD run on the same device. No flaps are seen after removing BFD.

  On Cisco IOS Release XE 3.6.0S, REP can run on the same device as BFD if configured with default timers. Flaps are seen only with fast-hellos on REP.

- CSCtw53121

  Symptoms: ES+ goes into major state occasionally on reload or SSO.

  Conditions: This issue is seen in the Cisco 7600 router with 40 gig ES+ line card that is running Cisco IOS Release 15.2(2)S.

  Workaround: There is no workaround.

- CSCtw70298

  Symptoms: Router crashes after the router bootup.

  Conditions: This symptom is seen with L2VPN xconnect.

  Workaround: There is no workaround.

- CSCty12641

  Symptoms: CFM ethernet ping fails with Cisco 7600 as the remote MEP end.

Conditions: This symptom is observed on a remote CFM over Xconnect MEPs with MEPs terminating on Cisco 7600 and having ESM20 line card.

Workaround: There is no workaround.

- CSCty16119

  Symptoms: MAC withdrawal does not happe.n

  Conditions: This symptom happens on shutting the VFI's VLAN on NPE. Failure of the spoke VC will work as expected.

  Workaround: Fail only the spoke VC without affecting the VFI and core VCs on NPE1.

- CSCty23747

  Symptoms: MAC Address withdrawal messages are not being sent.

  Conditions: This symptom is seen with flapping REP ports on UPE.

  Workaround: There is no workaround.

- CSCty26334

  Symptoms: The OSPFv3 neighborship between PE routers does not come up when sham-link is configured between the PE router. The problem is that VRF id of packet and VRF id of interface, on which packet is received (interface VRF1021) matches and therefore OSPF does not know it is sham-link packets and tries to associate it with process on this strange interface VRF1021. But there is no process on VRF1021.

  Conditions: This is observed only when trying to establish sham-link in SUP720.

  Workaround: There is no workaround

- CSCty28914

  Symptoms: CPU hog and CHUNKSIBLINGSEXCEED are observed followed by ES+ cash after performing line card OIR.

  Conditions: This symptom is observed after performing line card OIR of ES+ which is having scaled hardware offload BFD sessions.

  Workaround: There is no workaround.

- CSCty30952

  Symptoms: QoS policy-map gets rejected on shut/no shut of the interface or router reload.

  Conditions: This symptom occurs on router reload or shut/no shut of the interface.

  Workaround: Apply the policy-map back.

- CSCty45348

  Symptoms: DM in the port-shaper does not affect the police percent.

  Conditions: This symptom occurs when configuring a policy-map with shape in the egress direction. Do the DM and modify the rate. Policer changes do not work after the changes.

  Workaround: Have an absolute policer to ensure that we will not run into this problem. Dynamic modification of the policer might also fix the issue.

- CSCty46928

  Symptoms: The PIM SM mode is not supported for DATA-MDT groups.

  Conditions: This symptom is seen with PIM SM mode configuration for Data MDT groups and traffic stream with rate greater than mdt threshold to switch the traffic stream to Data MDT from default.

Workaround: There is no workaround.

- CSCty47231

  Symptoms: Traffic drops on removing the port-shaper.

  Conditions: Issue seen only when the policymap attach / detach is coupled with a link up/down, not seen on normal attach/detach. No issues with reload; policymap attached, and detached.

  Workaround: Default the egress interface and reconfigure. Traffic recovers.

- CSCty67401

  Symptoms: When traffic arriving on the ingress EVC BD interface is priority-tagged, the vlan id or priority value of traffic egressing out of EVC with double-encap or single-encap configuration respectively, gets incorrectly set to 0.

  Conditions: On a Cisco ME 3600X or ME 3800X that is running Cisco IOS Release 15.2(2)S, the CoS value of packet going out of EVC BD port with single-encap and vlan id of packet going out of EVC BD with double-encap are incorrectly set to 0.

  Workaround: There is no workaround.

- CSCty76106

  Symptoms: Crash after 2days of soak with traffic.

  Conditions: This symptom occurs with node acting as ConPE with multiple services like REP, MST, L3VPN, L2VPN, and constant frequent polling of SNMP, RCMD, full scale of routes and bidirectional traffic.

  Workaround: There is no workaround.

- CSCty77098

  Symptoms: Gig ports go DOWN.

  Conditions: This symptom occurs with different states during the EDVT testing.

  Workaround: There is no workaround.

- CSCty82786

  Symptoms: After removing and adding VLAN to the database, MAC Limit Shutdown does not work any more.

  Conditions: The issue is only seen after removing and adding VLAN to the database.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 15.2(2)S

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

- 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.

- CSCsh39289

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

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

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

- CSCsj23805

  Symptoms: RP crashes when issuing the **show ip eigrp timer** command.

  Conditions: This symptom happens on DMVPN HUB with scaling of more than 2000 spokes.

  Workaround: There is no workaround.

- CSCta27224

  Symptoms: This is a sister defect to CSCta27210 to add CLI support for cell payload scrambling on SPA-1CHOC3-CE-ATM. Currently, cell payload scrambling is off by default for ATM DS1 interfaces on SPA-1CHOC3-CE-ATM and on for E1 interfaces. Cell payload scrambling is currently not configurable. This presents an issue when connecting to ATM copper T1 CPEs that require cell payload scrambling or when connecting to E1s devices that do not support cell payload scrambling. As such, this defect makes cell payload scrambling configurable (on or off) on the ATM CEOP family of SPAs for all media types including:

  - SPA-1CHOC3-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1)
  - SPA-2CHT3-CE-ATM (ATM DS3)
  - SPA-24CHT1-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1)

  Conditions: This symptom is observed when using ATM or IMA DS1 T1 or E1 on any of the following:

  - SPA-1CHOC3-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1)
  - SPA-2CHT3-CE-ATM (ATM DS3, ATM E3)
  - SPA-24CHT1-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1)

  Workaround: There is no workaround.

- CSCta27728

  Symptoms: A Cisco router may crash.

Conditions: This symptom is observed on a Cisco ASR1002 router running Cisco IOS Release 15.1(2)S1 with RSVP for MPLS TE tunnel signaling.

Workaround: There is no workaround.

- CSCtc96631

  Symptoms: Packet drops occur in downstream devices every 4ms burst from shaper.

  Conditions: The symptom is observed when shaping at high rates on very fast interface types with low memory buffer devices downstream.

  Workaround: Use Cisco ASRs instead of Cisco ISRs.

- CSCtd87072

  Symptoms: IOSD restart seen.

  Conditions: The symptom is observed when changing tunnel mode on scaled IPSec sessions.

  Workaround: There is no workaround.

- CSCte96453

  Symptoms: Switch intermittently crashes when configuring energywise features.

  Conditions: The symptom is observed when the port is configured with “energywise level 10” to bring up a previously down port.

  Workaround: 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.

- CSCth08962

  Symptoms: A single bit error in the SRAM of the ATM SPA will generate the following error message:

  EST5EDT,M3.2.0/: spa_atm_v2[241]: SPA ATM4/2 SAR: An error was reported by SAR firmware (unsolicited msg): Description: Single-bit SRAM ECC correctable error. [Error code 4]

  It does not cause an operation impact, but the error message will repeat every 6 seconds.

  Single bit correctable errors should be counted but not display an error message since the information is already corrected by parity. Also, the rate of these messages may increase during certain conditions, which may choke the queues on the platform.

  Conditions: This symptom occurs under normal operating conditions.

  Workaround: There is no workaround.

- 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.

- CSCti48483

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

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

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

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml

- CSCti66155

  Symptoms: A Cisco IPSec router may unexpectedly reload due to bus error or software-forced crash because of memory corruption or STACKLOW error.

  Conditions: This is seen when the WAN link goes down and causes recursion between multiple tunnels using tunnel protection. (That is, there are tunnel 0 and tunnel 1. After the WAN link goes down, the routing table shows a link to the tunnel 0 destination through tunnel 1 and the tunnel 1 destination is through tunnel 0.)

  Workaround 1: Change the tunnel source to be the physical WAN interface so that when the WAN link does go down, the tunnels are brought down immediately.

  Workaround 2: Change the routing protocol so that the router in question does not have recursive routing when the link goes down.

  Workaround 3: If possible, create a floating null route for the tunnel destinations that is less preferred than the route normal route to the tunnel destination, but more preferred than the route that gets installed after the WAN link goes down.

- CSCti67832

  Symptoms: Cisco 3900e platform router reloads while try to enable GETVPN Group Member (GM) all-features debugs.

  Conditions: The symptom is observed on a Cisco 3900e router that is running Cisco IOS interim Release 15.1(2.7)T and while trying to enable the debug **debug crypto gdoi gm all-features**.

  Workaround: There is no workaround.

- CSCtj05903

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

  Conditions: This symptom occurs on scaled sessions.

  Workaround: There is no workaround.

- CSCtj06390

  Symptom: Ping fails after configuring crypto.

Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 15.1(2.18)T.

Workaround: There is no workaround.

- CSCtj10592

  Symptoms: DVTI GRE IPv4 mode fails to create virtual-access for IKEv2 connections.

  Conditions: The symptom is observed with a simple SVTI to DVTI connection.

  Workaround: There is no workaround.

- CSCtj14525

  Symptoms: Standby is not synced to active after attaching a new policy.

  Conditions: This symptom happens when dynamic policy is used such as RADIUS CoA.

  Workaround: There is no workaround.

- CSCtj30238

  Symptoms: WRED counters are wrongly updated. The default counter should be 0, but the counter is wrongly updated. All the WRED subclasses show the same count. Counters are shown for WRED subclasses for which there are no traffic matches in the class.

  Conditions: This issue is seen on the Cisco 7600 router with ES+ line card only. The Es+ line card does not support per WRED class based counters. There was a recent breakage due to the Transmit packets/bytes column that started showing up for the Es+ line card. This is wrong. As ES+ writes same value to WRED transmit count (not the per subclass base count, but total count), this value does not make sense.

  Workaround: Do not use WRED subclass Transmit packets/bytes counters for ES+ line card on the Cisco 7600 router.

- CSCtj38234

  Symptoms: IPSec IKEv2 does not respond to INVALID_SPI informational message. It should respond with another INFORMATIONAL IKE message.

  An INVALID_SPI may be sent in an IKE INFORMATIONAL exchange when a node receives an ESP or AH packet with an invalid SPI. The notification data contains the SPI of the invalid packet. The INVALID_SPI message is received within a valid IKE_SA context.

  Conditions: The symptom is observed when an IKEv2 peer sends an INFORMATIONAL IKE message notifying about an INVALID_SPI (IPSec).

  Workaround: There is no workaround.

- 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 subinterface 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.

- CSCtj76297

  Symptoms: Router hangs with interoperability of VM and crypto configurations.

  Conditions: The symptoms are seen only during interoperability between video-monitoring and crypto (IPSec VPN) with an AIM-VPN/SSL-3 card.

  Workaround: Disable AIM and use onboard CE.

- CSCtj78966

  Symptoms: A Cisco ASR 1000 router crashes with thousands of IKEv2 sessions, after many operations on IKEv2 session.

  Conditions: This symptom is seen when IKEv2 SA DB WAVL tree is getting corrupted if we fail to insert the SA due to some error, for example, PSH duplication.

  Workaround: There is no workaround.

- CSCtj79368

  Symptoms: All keyservers crash after removing RSA keys before changing to new ones based on security concerns.

  Conditions: The symptom is observed when removing RSA keys.

  Workaround: Stay on the same RSA keys.

- CSCtk03371

  Symptoms: SVI-based EoMPLS/VPLS VC fails to forward traffic even when VC is up.

  Conditions: This happens when the **ip cef accounting non-recursive** command is configured on the router. This command is documented as an unsupported command on the Cisco 7600 platform, but it should also generate an error message when configured on the Cisco 7600. Preferably it should not take any action, for example, it should not affect any other working features.

  Workaround: Unconfigure the command by typing “no ip cef accounting non- recursive”.

- CSCtk15360

  Symptoms: xauth userid mode http-intercept does not prompt for a password and the Ezvpn session does not come up.

  Conditions: This symptom occurs when the EzVPN client, x-auth is configured as http-intercept.

  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.

- CSCtk69114

  Symptoms: RP resets while doing ESP reload with crypto configuration.

  Conditions: This symptom is observed by unconfiguring and configuring interface configuration and reloading both ESPs. The RP crashes on the server.

Workaround: There is no workaround.

- CSCtl20993

  Symptoms: Router crashes during IPsec rekey.

  Conditions: The conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtl23748

  Symptoms: EoMPLS over GRE (DMVPN) with IPSec protection is not working after a reboot.

  Conditions: The symptom is observed when there is a tunnel (Ethernet over MPLS over GRE over IPSec) between PE1 and PE2 and following a reload and when tunnel protection is configured.

  Workaround: There is no workaround.

- CSCtl77241

  Symptoms: The switch crashes following webauth, as AAA accounting begins.

  Conditions: This symptom occurs under the following conditions:

  – Webauth is used.
  – AAA accounting is enabled for proxy-auth.

  Workaround: Disable AAA accounting.

- 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.

- CSCtn02372

  Symptoms: QoS installation fails on the CEoP SPA or traffic is not forwarded correctly after a lot of dynamic changes that continuously remove and add VCs, as on CEoP SPA, IfIDs are not freed upon deleting the PVC.

  Conditions: This symptom occurs when continuous bring-up and tear down of VCs causes the SPA to run out of IfIDs.

  Workaround: Reload the Cisco SIP-400 line card.

- CSCtn07696

  Symptoms: The Cisco 6506-E/SUP720 may crash while redirecting the **show tech-support** command output using the **ftp** command due to TCP-2-INVALIDTCB.

  Conditions: This symptom is observed with the following CLI:

  ```
  show tech-support | redirect
  ftp://cisco:cisco@10.0.255.14/Cisco/tech-support_swan21.pl.txt
  ```

  During the FTP operation, if the interface fails or shuts down, it could trigger this crash.

  Workaround: This is an FTP-specific issue. Redirect the output by TFTP or other protocols.

- CSCtn12119

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

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

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

- CSCtn16855

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

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

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

- CSCtn18229

  Symptoms: A policy does not get suspended.

  Conditions: This symptom is observed if a policy is applied to fr-pvc, then the member link is flapped from the peer for mfr subint.

  Workaround: There is no workaround.

- CSCtn22728

  Symptoms: See the following:

```
Router(config)#monitor session 1 type erspan-source
Router(config-mon-erspan-src)#destination ?
  <cr>

Router(config-mon-erspan-src)#destination int g11/48
Router(config-if)#
Config Sync: Line-by-Line sync verifying failure on
command:
  destination int g11/48
due to parser return error
```

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

  Workaround: Do not issue not applicable commands.

- CSCtn26750

  Symptoms: The standby RP reloads due to a config-sync error.

  Conditions: The symptom is observed when “authentication” or “encryption” is configured for an OSPFv3 virtual link. Then it is changed to use a different SPI, but IPSec fails to remove the policy for the old SPI. When it is changed back to the old SPI, the command fails with the error:

```
%OSPFv3-3-IPSEC_POLICY_ALREADY_EXIST: SPI is already in use with ospf process
```

  On the active RP the “virtual-link ipsec” configuration is removed, but on the standby RP it remains. Reconfigure “virtual-link ipsec” using the second SPI. This command succeeds on the active RP so it is synched to the standby, however the command already exists on the standby so it generates the config- sync error and reloads.

  Workaround: Instead of simply changing the SPI from X to Y, remove X using a **no** command and then configure Y.

- CSCtn39632

  Symptoms: RSA key cannot be configured under a keyring any more. The RSA key will be configured in global configuration.

  Conditions: This occurs on a Cisco ASR 1000 series router configured for RSA key encryption with a keyring name having more than 8 characters.

  Workaround: Modify the keyring name to be less than 8 characters.

- CSCtn39950

  Symptoms: An IPsec session will not come up.

  Conditions: This symptom occurs if a Cisco ISR G2 has an ISM VPN accelerator and slow interfaces such as BRI-PRI. Crypto plus ISM VPN module plus slow interfaces will not work.

  Workaround: Disable the ISM VPN module and switch to the onboard crypto engine.

- 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.

- CSCtn59075

  Symptoms: A router may crash.

  Conditions: This has been experienced on a Cisco router that is running Cisco IOS Release 15.1(3)T, 15.1(3)T1, and 15.1(4)M. Flexible NetFlow needs to be running.

  Workaround: Disable Flexible NetFlow on all interfaces.

- CSCtn70367

  Symptoms: IPSEC key engine crashes at sessions setup.

  Conditions: This symptom is seen when setting up sessions with the configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. The crash happens on IPSEC key engine. The crash occurs while UUT is establishing SAs that are requested. This issue is reproduced by clear crypto session on CES after all SAs are established.

  Workaround: There is no workaround.

- CSCtn79475

  Symptoms: A Cisco router reloads often due to stack overflow under some traffic conditions.

  Conditions: This symptom is observed when calls resulting in VOIPRTP media loop are seen.

  Workaround: There is no workaround.

- CSCtn83520

  Symptoms: VOIP_RTCP related traceback is seen.

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

  Workaround: There is no workaround.

- CSCtn95395

  Symptoms: VTEMPLATE Background Mgr crashes on DVTI server after using the **clear crypto session** command on DVTI client.

Conditions: This symptom is seen on DVTI server when sessions are setting up with the IPSec DVTI configuration of 1000 VRFs, one IKE session per VRF, and four IPSec SA dual per session. We might run into VTEMPLATE Background Mgr process crashing after executing the **clear crypto session** command a couple of times on DVTI client.

Workaround: There is no workaround.

- CSCto10336

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

  Conditions: This symptom occurs during control channel cleanup.

  Workaround: There is no workaround. This symptom can be only removed through power cycle.

- CSCto10485

  Symptoms: With a GRE over IPSec configuration using tunnel protection, traffic originated from the router may be dropped on the receiving router due to replay check failures. This is evident by the %CRYPUO-4-PKT-REPLAY drops as shown in the syslog.

  Conditions: This issue typically occurs during high traffic load conditions.

  Workaround: There is no workaround.

- CSCto12825

  Symptoms: The multilink policy cannot be removed.

  Conditions: This symptom is observed with MPOL configured; when multilink goes to suspension, the policy cannot be removed.

  Workaround: There is no workaround.

- CSCto31255

  Symptoms: Router crashes at fair-enqueue.

  Conditions: The symptom may be seen on Cisco 5400 and 7200 platforms.

  Workaround: There is no workaround.

- CSCto60216

  Symptoms: Cisco IOS crashes in ospfv3_write.

  Conditions: This symptom occurs when the **issu runversion** command is entered multiple times within a short period of time.

  Workaround: Wait for the newly active router processor to completely initialize.

- CSCto61736

  Symptoms:

  1. NBAR remains enabled in CEF path.
  2. Packet counters not incrementing in “show adjacency lisp0 detail”.
  3. ADQ/PD not working on ATM-subinterface and frame-relay subinterfaces.
  4. **ip nbar port-map** CLI is broken.

  Conditions:

  1. The symptoms 1 and 2 are observed when NBAR is enabled and disabled on the interface.
  2. Symptoms 3 and 4 are seen when the configuration/show CLIs are executed.

  Workaround: There is no workaround.

- CSCto70125

  Symptoms: IP SLA TCP connect probe is configured via SNMP, then IP SLA Event Processor process goes to 100% CPU.

  Conditions: This issue is seen for TCP connect probes. The issue may affect multiple Cisco IOS releases but has been observed on Cisco IOS Releases 12.2 (33)SXH and 12.2(33)SXI based releases.

  Workaround: Set up probe via CLI.

- 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.

- CSCto72350

  Symptoms: A stale suspended service-policy remains.

  Conditions: This symptom is observed when the policy CLI is removed when policy is suspended.

  Workaround: There is no workaround.

- CSCto72629

  Symptoms: A MAXAGE LSA is repeatedly retransmitted bringing down the OSPFv3 adjacency.

  Conditions: This symptom occurs when the unadjusted age of the LSA in the OSPFv3 database (as opposed to the advertised age, which includes time spent in the database) is less than MAXAGE. Note that the age of the LSA in the database is not updated once it is installed unless maxaging is initiated by OSPFv3 process.

  Workaround: Use the **clear ipv6 ospf process** command to clear the OSPF state based on the OSPF routing process ID.

- CSCto72927

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

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

  Workaround: There is no workaround.

- CSCto73151

  Symptoms: The RP resets.

  Conditions: This symptom occurs when the **show ip nhrp** command is issued to check mixed DMVPN and SVTI.

  Workaround: There is no workaround.

- CSCto73345

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

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

  Workaround: There is no workaround.

- CSCto85731

  Symptoms: Crash seen at the nhrp_cache_info_disseminate_internal function while verifying the traffic through FlexVPN spoke-to-spoke channel.

  Conditions: The symptom is observed under the following conditions:

  1. Configure hub and spokes (flexvpn-nhrp-auto connect) as given in the enclosure.
  2. Initiate the ICMP traffic through spoke-to-spoke channel between spoke devices.
  3. Do a **clear crypto session** at Spoke1.
  4. Repeat steps 2 and 3 a couple of times.

  Workaround: There is no workaround.

  Further Problem Description: In the given conditions, one of the spoke device crashed while sending ICMP traffic (10 packets) through FlexVPN spoke-to- spoke channel. The crash decode points to “nhrp_cache_info_disseminate_internal” function

- CSCto90252

  Symptoms: A standby route processor (RP) is stuck to “init, standby” for about 10 hours.

  Conditions: This symptom occurs after reloading five or six times on a Cisco ASR 1000 series router.

  Workaround: Disable NSR.

- CSCto92529

  Symptoms: Unable to configure “ipv6 ospf authentication ipsec spi 7000 md5 <>”.

  Conditions: The symptom is seen on Cisco routers loaded with Cisco IOS interim Release 15.2(2.11)T.

  Workaround: There is no workaround.

- CSCtq10684

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

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

  Workaround: A possible workaround is to reload the box.

- CSCtq23793

  Symptoms: After reloading PE router in mVPN network, multicast traffic stops on one of the VRFs randomly.

  Condition: This symptom occurs under the following conditions:

  -When reloading a PE in mVPN network. -When PE has many VRFs and scaled mVPN configuration.

  Workaround: Remove and add MDT configuration.

- CSCtq24006

  Symptoms: DMVPN tunnels will not come up with an IPv6 address.

  Conditions: This symptom is observed if more than one tunnel is present on the spoke.

  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.

- CSCtq32282

  Symptoms: Chunk leaks observed on various platforms.

  Conditions: The issue seen while testing the ipsec_unity_solaris functionality.

  Workaround: There is no workaround.

- CSCtq37579

  Symptoms: Enabling and disabling “snmp-server traps” crash the UUT.

  Conditions: The symptom is observed when you disable the snmp-server and do a **write memory**.

  Workaround: There is no workaround.

- CSCtq39602

  Symptoms: DMVPN tunnel is down with IPSec configured. The **show dmvpn** command from the spoke shows the state is IKE.

  Conditions: After heavy traffic was pumping from DMVPN hub to spoke for some time: from a few minutes to a couple of hours.

  Workaround: Configuring “crypto ipsec security-association lifetime kilobytes disable” to disable volume-based rekeying will reduce the problem.

- CSCtq47856

  Symptoms: The following issues are observed:

  1. Crypto map is configured with a local ACL at registration time.
  2. Local ACL is removed from global configuration (without removing it from the crypto map configuration).
  3. Remove crypto map from the interface.

     Issue 1: At this point **show crypto gdoi** continues to display the TEK SA, even though the GM has no interfaces configured with a crypto map.
  4. Reapply the crypto map to the interface and let registration complete.

     Issue 2: If **crypto gdoi ks rekey** is issued on the keyserver, then **show crypto gdo** continues to display only the old TEK. New TEKs installed by subsequent rekeys are not displayed.
  5. On the keyserver, issue **crypto gdoi ks rekey replace**.

     Issue 3: GM crashes in the IPSec code while processing the new SAs and shortening the old ones.

  Conditions: The symptom is observed on a router that is running GET VPN.

  Workaround: Remove the ACL from the crypto map configuration before removing it from the global configuration.

- 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”.

- CSCtq61128

  Symptoms: Router is crashing with segmentation fault (11).

  Conditions: This symptom is observed on routers acting as IPSEC hub using certificates.

  Workaround: There is no workaround.

- CSCtq63225

  Symptoms: Packet drop seen when running traffic.

  Conditions: The symptom is observed when IPSec along with QoS is configured.

  Workaround: There is no workaround.

- CSCtq63487

  Symptoms: The next set action is not executed with multi-action policy Routemap when set VRF fails.

  Conditions: This symptom occurs when deleting VRF, which causes a problem when other set clause is configured with set VRF.

  Workaround: There is no workaround.

- CSCtq69083

  Symptoms: Nested IPSec tunnel with outer tunnel GRE and inner tunnel VTI/GRE is not working.

  Conditions: The symptom is observed with the v150-1.M4.6 image.

  Workaround: There is no workaround.

- CSCtq75008

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

  Conditions:

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

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

  Workaround: There is no workaround.

- CSCtq75045

  Symptoms: When a router is running FlexVPN-IKEv2 in auto-reconnect mode, IPSec SAs are not renegotiated properly after a **clear crypto session** command is entered. Entering the **show crypto ikev2 client flexvpn** command will indicate that the router is in a NEGOTIATING state.

  Conditions: This symptom is observed on a router running FlexVPN on IKEv2 in auto-reconnect mode.

  Workaround: Enter the **clear crypto ikev2 client flexvpn** command to clear the FlexVPN state and renegotiate the SAs successfully.

- CSCtq79382

  Symptoms: In the HA setup and on the Active, if you have a probe configured with VRF and you remove the VRF with **no ip vrf** *vrfname* and reboot, it keeps rebooting again and again (crashes).

  Conditions: The symptom is observed when removing the VRF and rebooting the Active terminal.

  Workaround: Check that the system is in standby and that there is no VRF configured. Even though there is a probe configured with VRF, you can proceed without crashing the Active after a reboot.

- CSCtq79767

  Symptoms: IPSEC key engine crashes after using the **clear crypto session** command on CES.

  Conditions: This symptom occurs under the following conditions:

  1. Topology:

     IXIA --> CES (DVTI Client) --> UUT (DVTI Server)-->

  2. Configuration:

     1000 vrf x 1 IKE session x 4 IPsec SA dual

  3. The crash on UUT is seen after using the **clear crypto session** command on CES after all SAs have been established.

  Workaround: There is no workaround.

- CSCtq83601

  Symptoms: EoMPLS traffic does not flow after MPLS TE tunnel path change after FRR.

  Conditions: This symptom occurs under the following conditions:

  - The TE tunnel is used as PW.
  - The VC does not flap and label stack looks fine.

  This issue is seen only with port-based xconnect.

  Workaround: Shut/no shut the AC interface to try and resolve the problem.

- CSCtq84313

  Symptoms: Router hangs and then crashes due to watchdog timer expiry.

  Conditions: This symptom is observed when IP SLA probes are configured, and then the configuration is replaced with one that has no IP SLA probes.

  Workaround: Reset the ip sla.

- CSCtq88777

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

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

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

- CSCtq92940

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

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

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

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

- 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.

- CSCtr01431

  Symptoms: An error is encountered during configuration synchronization.

  Conditions: This issue is observed when the following sequence of steps is performed:

  1. A loopback interface is created
  2. The macro interface range is configured for the loopback interface.
  3. The loopback interface is deleted.
  4. SSO is performed.

  Workaround: There is no workaround.

- CSCtr07142

  Symptoms: A memory leak is seen at crypto_ss_open.

  Conditions: No special configuration is needed.

  Workaround: There is no workaround.

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

- 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.

- CSCtr14675

  Symptoms: The line card crashes after removing the child policy in traffic.

  Conditions: This symptom occurs after the child policy is removed in traffic.

  Workaround: There is no workaround.

- CSCtr16857

  Symptoms: Windowing in IKEv2 is broken.

  Conditions: This symptom occurs when an error condition in AUTH exchange causes the delete message to not be sent because of incorrect windowing. The following error is seen:

  ```
  "No room in peer window request is throttled: Current Req = 2 Next Req = 1"
  ```

  Workaround: There is no workaround.

- CSCtr20300

  Symptoms: SA negotiation test is failing for ipsec_core script.

  Conditions: The symptom is observed when the SA should come into idle state after using "show crypto isakmp sa".

  Workaround: There is no workaround.

- CSCtr21296

  Symptoms: The following messages are seen continuously on the router console:

  ```
  [ipsec_dp_expand_sa]Invalid data cipher info
  [ipsec_dp_expand_action]No memory to allocate SA for decrypt action
  ```

Conditions: The issue is seen after disabling the hardware crypto engine.

Workaround: There is no workaround.

- CSCtr23134

  Symptoms: Crash seen when IKEv2 debugs are enabled.

  Conditions: The symptom is observed when using the debug “debug crypto ikev2 internal.”

  Workaround: There is no workaround.

- CSCtr24751

  Symptoms: Cisco ME 3600X BGP is flapping every 55 hours and 58 minutes on GE interface.

  Conditions: This symptom is seen with peer BGP neighbor and ingress numbers of BGP route from TenGE.

  Workaround: There is no workaround.

- CSCtr24889

  Symptoms: Adding a second static route in a VRF and then removing it causes a traceback.

  ```
  %MPLS_IPRM-3-INTERNAL: x.x.x.x/32 (vrfname(86)); prefix path set from outinfo,
  illegal outinfo type: 4
  -Traceback= 62A306AC 62A30908 62A30E08 62A33D20 62A33F98 60470B78 60476644 604B8440
  604B8690 604BCE00 604BCF68 6056B5F0 6056B744 610E9EA8 610DDC68 610E009C
  ```

  Conditions: This symptom occurs when adding a second static route in a VRF and then removing it.

  Workaround: There is no workaround.

- CSCtr25127

  Symptoms: When switching between ATM and 3G interfaces, the following traceback is observed.

  ```
  %ALIGN-3-CORRECT: Alignment correction made at 0x23D242DCz reading 0xE85C77B
  %ALIGN-3-TRACE: -Traceback= 0x23D242DCz 0x23CDE700z 0x23CFDF50z 0x225C0594z
  0x225C1368z 0x22DD4564z 0x21F88D28z 0x2173449Cz
  %ALIGN-3-CORRECT: Alignment correction made at 0x23D2430Cz writing 0xE85C77B
  %ALIGN-3-TRACE: -Traceback= 0x23D2430Cz 0x23CDE700z 0x23CFDF50z 0x225C0594z
  0x225C1368z 0x22DD4564z 0x21F88D28z 0x2173449Cz
  ```

  Conditions: This symptom is observed when switching between ATM and 3g interfaces.

  Workaround: There is no workaround.

- CSCtr25386

  Symptoms: BFDv6 static route association fails after reenabling interfaces.

  Conditions: This symptom is observed after interfaces are reenabled.

  Workaround: There is no workaround.

- CSCtr30121

  Symptoms: Delayed Offer to Early Offer calls that go through CUBE may not be communicated properly between CUBEs in an HA environment. The result could be no audio on failover.

  Conditions: This symptom is seen when using CUBE HA.

  Workaround: There is no workaround.

- CSCtr31153

  Symptoms: Packet decryption seems to fail with manual crypto maps configured on interface.

Conditions: The symptom is observed on a Cisco 7200 series router loaded with Cisco IOS interim Release 15.2(0.19)T0.1.

Workaround: There is no workaround.

- CSCtr31496

  Symptoms: The line card crashes after switchover with the multilink configurations.

  Conditions: This symptom occurs after switchover with the multilink configurations.

  Workaround: There is no workaround.

- CSCtr34960

  Symptoms: A router that is running Cisco IOS may run out of IO memory.

  The **show buffers** command shows that the count reaches 0 in free list.

```
Router#sh buffers
...
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
....
```

  Conditions: This issue is seen post bootup. The Cisco 7600 in HA is required to hit the issue. The **show buffers old** command shows some buffers hanging on EOBC buffers list for a long time, weeks or more. The issue is a corner case, and buffer leak rate is slow.

  This DDTS fixes leaks for the **mls cef maximum-routes** and **mls cef adjacency-mcast** commands.

  See the output from the **show buffers old pack**:

```
F340.08.04-6500-2-dfc1#show buf old packet

Buffer information for EOBC0/0 buffer at 0x275A0B00
  data_area 0x275A0FB8, refcount 1, next 0x0, flags 0x0
  linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
  if_input 0x273AF610 (EOBC0/0), if_output 0x0 (None)
  inputtime 00:00:02.764 (elapsed 00:16:36.380)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x275A100C, datagramsize 50, maximum size 1680
  mac_start 0x275A0FFE, addr_start 0x275A0FFE, info_start 0x0
  network_start 0x275A100C, transport_start 0x0, caller_pc 0x205DF718

275A100C: 00200000 02010000 00010006 01000000  . ..............
275A101C: 00350001 00101608 00000053 000000A6  .5.........S...&
275A102C: 000603E7 01170000 00000000 00000000  ...g............
```

```
          --------
275A103C: 000000                                ...

Buffer information for EOBC0/0 buffer at 0x275A5B48
  data_area 0x275A6000, refcount 1, next 0x0, flags 0x0
  linktype 69 (IPC), enctype 1 (ARPA), encsize 14, rxtype 0
  if_input 0x273AF610 (EOBC0/0), if_output 0x0 (None)
  inputtime 00:00:02.764 (elapsed 00:16:41.380)
  outputtime 00:00:00.000 (elapsed never), oqnumber 65535
  datagramstart 0x275A6054, datagramsize 80, maximum size 1680
  mac_start 0x275A6046, addr_start 0x275A6046, info_start 0x0
  network_start 0x275A6054, transport_start 0x0, caller_pc 0x205DF718


275A6054:          00200000 02010000 02150007      . ..........
275A6060: 01000000 000A0001 00301608 00000052  .........0.....R
275A6070: 000000A4 00480002 01047FFF 00000001  ...$.H..........
                   --------
275A6080: 00000000 00000000 00000000 00000000  ................
275A6090: 00000001 00000000 00000000 00000000  ................
275A60A0: 00000000 00

F340.08.04-6500-2-dfc1#
```

The **show buffers old packet** command output will be either 000603E7 OR 00480002.

Workaround: Reload the supervisor to clear the leaked buffers.

- CSCtr35740

  Symptoms: QoS queuing hierarchy not moved to current active link when the previously active link goes down.

  Conditions: The symptom is observed when the DMVPN tunnel active link goes down.

  Workaround: There is no workaround.

- CSCtr42341

  Symptoms: Crash at task_execute_prep.

  Conditions: The symptom is observed with a Cisco 800 series router that is configured with BFD.

  Workaround: There is no workaround.

- CSCtr42913

  Symptoms: Stale crypto maps seen even after unconfiguring tunnel protection.

  Conditions: The symptom is observed when removing the tunnel source configuration.

  Workaround: Unconfigure and configure again or unconfigure tunnel protection first.

- CSCtr46854

  Symptoms: The PPP multilink between the Cisco ISR G2 router and the Cisco ASR 1000 router crashes the Cisco ISR router.

  Conditions: This symptom is observed with the Cisco ISR G2 router.

Workaround: Remove authentication on the Serial interface on the Cisco ASR router.

- 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.

- CSCtr48525

  Symptoms: When “medium p2p” is configured under a physical interface, followed by configuration of the “mpls tp link” with a unicast entry for tx-mac (in that order) and then by “no medium p2p”, the “mpls tp link” entry is removed from the interface configuration without notification. Removal of the “mpls tp link” entries based on changes in the interface P2P status via the “medium p2p” configuration is inconsistent.

  Conditions: This symptom is observed in an IPLess configuration. First, “medium p2p” is added under a physical interface, followed by configuration of the “mpls tp link” with a unicast entry for tx-mac. Then, “medium p2p” is removed from under that physical interface. It is seen that the configuration for “mpls tp link” with a unicast entry for tx-mac is also removed from under the physical interface without notification to the user.

  Workaround: There is no workaround.

- CSCtr51926

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

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

  Workaround 1: Enable IPv6 explicitly on the main interface:

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

  Workaround 2: Reconfigure the IPv6 address on the subinterface:

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

- CSCtr52740

  Symptoms: Query on an SLA SNMP MIB object using an invalid index can cause the device to crash.

Conditions: The symptom is observed when querying history information from rttMonHistoryCollectionCompletionTime object using invalid indices.

Workaround: Instead of using “get”, use “getnext” to list valid indices for the MIB OID.

- CSCtr53056

  Symptoms: The Cisco ME 3600 crashes due to watchdog timeout.

  Conditions: This symptom occurs when switchport is configured on an interface that has PIM enabled. This is a timing issue and may not be seen every time.

  Workaround: There is no workaround.

- CSCtr53739

  Symptoms: The tunnel-encap entry is wrongly programmed. The following **show** command is used:

  show platform software multicast ip cmfib vrf *vrf- name* **tunnel-encap verbose**

  Conditions: This symptom occurs during deletion and readdition of the VRF with the multicast MDT configured and P2P tunnels as the access-facing interface, along with Gigabit subinterfaces.

  This issue is seen under the following conditions:

  1. Configure the mcast VRF with P2P tunnels as access-facing, along with Gigabit subinterfaces. Use a sip400 line card as the access-facing line card.
  2. Delete the VRF, P2P tunnel, and Gigabit subinterface.
  3. Add the same VRF again after a 60-second interval.
  4. Observe the tunnel-encap entry wrong programmed on the SP, with corrupt values.

  Workaround: There is no workaround.

- CSCtr56174

  Symptoms: The MPLS-TE link count reaches a large value (4 billion+) on the Cisco ASR 1000 series router and negative value on the Cisco 7600 series router. This issue is seen in the **show mpls tr link sum** and **show mpls tr link int** command output.

  Conditions: This symptom occurs if MPLS-TE tunnels are deleted using the **no int tunX** command and if the number of TE tunnels deleted are more than the TE links on the box. Even if they are not, with every TE tunnel deleted, the link count is affected and gets reduced.

  Workaround: Do not delete MPLS-TE tunnels using the **no int tuX** command. If a TE tunnel is not required, shut it down. If these symptoms are observed, the only way is to reboot.

- CSCtr59314

  Symptoms: A router reloads when the **clear crypto session** command is issued with 4000 sessions up.

  Conditions: This symptom is observed only under load conditions.

  Workaround: There is no workaround.

- CSCtr61289

  Symptoms: FlexVPN client remains in NEGOTIATING state, despite being on auto- connect mode, when the FlexVPN server executes a **clear crypto session**.

  Conditions: This occurs in a dVTI setting, where the server has a virtual- template interface and the client has a static tunnel interface that connects to the server. This is not observed in a static setting.

  Workaround: On the client, issue a **clear crypto ikev2 client flexvpn** to clear the FlexVPN session and allow the client to reconnect to the server again.

- CSCtr61623

  Symptoms: The RP crashes at _be_ace_create_acl_node.

  Conditions: This symptom is observed when configuring the 4K DVTI VT.

  Workaround: There is no workaround.

- CSCtr67852

  Symptoms: Invalid route entries injected by the RRI mechanism after an HSRP failover happens in a stateful IPSec HA setup.

  Conditions: The symptom is observed following a failover in a stateful IPSec HA setup and the use of RRI.

  Workaround: Clear all crypto sessions with **clear crypto session** or remove and add back the crypto map to the interface where it is applied.

- CSCtr69416

  Symptoms: Configuring “redistribute connected” in OSPF does not work for some interfaces. Configuring “redistribute ospf” in other protocols works even if OSPF is not enabled on interfaces.

  Conditions: This symptom occurs under the following conditions:

  – Enable OSPF on the interface using the **ip ospf area** command.

  – Delete the OSPF process using the **no router ospf** command.

  This issue is seen if the OSPF process is reenabled and the interface is not a part of a new OSPF process anymore.

  Workaround: Use the **ip ospf area** and the **no ip ospf area** commands to reset internal flags.

- CSCtr72835

  Symptoms: The “Unable to initialize the geometry of nvram” message is coming continuously on the console while performing ISSU upgrade from Cisco IOS Release XE 3.4S to Release XE 3.5S.

  Conditions: This symptom is seen when performing ISSU upgrade from Cisco IOS Release XE 3.4S to Release XE 3.5S.

  Workaround: There is no workaround.

- CSCtr79347

  Symptoms: crashes at BGP Task without a BGP configuration change or BGP neighbor up/down event.

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


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

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

  Workaround: There is no workaround.

- CSCtr79905

  Symptoms: Error message seen while detaching and reattaching a service policy on an EVC interface.

Conditions: The symptom is observed when detaching and reattaching the service policy on an EVC interface when port shaper is configured on the interface.

Workaround: There is no workaround.

- CSCtr81559

  Symptoms: The PPP session fails to come up occasionally on LNS due to a matching magic number.

  Conditions: This symptom is observed during LCP negotiation, when the random magic number generated on the client matches the magic number generated on the LNS. PPP assumes it to be a loopback and disconnects the PPP session. This condition occurs rarely.

  Workaround: To avoid this, renegotiate the LCP. Configure the client using the **retry** command. This may cause the next session to come up correctly.

- CSCtr82351

  Symptoms: Router crashes when trying to change OSFP area/multipath parameters.

  Conditions: This symptom is seen when the NLFM learning process causes CPU HOG, and the router is forced to crash by watchdog.

  Workaround: There is no workaround.

- CSCtr82600

  Symptoms: More than half the amount of multicast traffic is dropped.

  Conditions: This issue is seen in scale condition when moving from data MDTs to default MDTs.

  Workaround: Clear all the mroutes in each VRF.

- CSCtr86149

  Symptoms: A router crashes if placing a call from an ISDN phone to an IP phone. The call is a secure SIP call (TLS); the phone is also using secure SCCP.

  Conditions: The router is in secure SRST mode due to a WAN outage.

  Workaround: There is no workaround.

- CSCtr86666

  Symptoms: EIGRP flap due to retry limit exceeded. On peer it is waiting for INIT ACK and complains of out of order sequence number.

  Conditions: DMVPN network with a spoke running Cisco IOS Release 15.1(4)M.

  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.

- CSCtr87740

  Symptoms: A router may crash due to a bus error.

  Conditions: The symptom seems to be related to high traffic and an ongoing rekey taking place.

  Workaround: There is no workaround.

- CSCtr88739

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

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

Conditions: The 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.

- CSCtr92285

  Symptoms: The following log is seen, and VCs cannot be configured.

  SSM CM: SSM switch id 0 [0x0] allocated ACLIB [Gi9/1/0.3830, 3830]: Failed to setup switching for VLAN interface ...

  Conditions: This symptom is observed with the access circuit interface shut and core flaps occurring, along with pseudowire redundancy. Also, leaks occur per flap.

  Workaround: There is no workaround. If VCs can be removed, do so to release some IDs. Otherwise, try a redundancy switchover.

- CSCtr93337

  Symptoms: A route-map for IPv6 is configured with set VRF action. After sending the traffic, VRF neighbor is not getting resolved.

  Conditions: This symptom is seen when IPv6 PBR is configured with set VRF part.

  Workaround: Before sending the traffic, resolve neighborship by sending ping or using BGP routing protocol.

- CSCtr93685

  Symptoms: SPA console is disabled and, interface goes up/down on executing the command for SPA keepalive failure.

  Conditions: This symptom is seen after executing the **slay -s SIGSEGV spa_ipc** command at the SPA console. The SPA is UP and the controller is UP. No alarms are seen at the controller output. All the serial interfaces go UP/DOWN on the local end, and at the remote end they are DOWN/DOWN.

  After this, unable to login on the SPA console. The issue is seen on the chopper spa also.

  Workaround: Reset the line card.

- CSCtr94545

  Symptoms: Standby crashes at fm_global_feature_add_for_vrf.

  Conditions: The system crashes when virtual servers are deleted.

  Workaround: There is no workaround.

- CSCts00341

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

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

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

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

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

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

- CSCts01653

  Symptoms: Spurious memory access seen on video monitoring router.

  Conditions: The issue is seen after recreating the interface.

  Workaround: There is no workaround.

- CSCts02627

  Symptoms: The **show mac-address-table** command displays invalid/incomplete port list for entries learned on VPLS Bridge Domain.

  It is observed that port-channel "Po1" is displayed as "Po", and the Virtual Circuit IDs are missing in the port list of the mac-address-table entries. This is a display issue.

  Conditions: This symptom is observed only with mac-address-table entries that are learned on VPLS Bridge Domain VLAN.

  Workaround: There is no workaround.

- CSCts05166

  Symptoms: A Cisco 7200 series router drops frame-relay LMI from third party if C/R bit is set to 1 in it. This further drops the frame-relay link.

  Conditions: This symptom is seen when frame-relay+other side is sending LMI with C/R bit 1 occasionally. Encapsulation frame-relay on Cisco can be Cisco or IETF. Both noticed the problem.

  Workaround: There is no workaround.

- CSCts06929

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

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

  Workaround: Configuring graceful restart resolves this issue.

- CSCts11594

  Symptoms: A mediatrace session is scheduled with an attached session- parameter. The session is unscheduled and the session-parameters removed so that the default session parameters should be used.

  On the first schedule, traceback is seen. The session is again unscheduled and scheduled for second time and a crash is seen.

  Conditions: The symptom is observed when using custom session-parameters for a session and then removing it. Then using the default session-parameters followed by scheduled and unscheduled twice.

  Workaround: Use either the default session-parameters or custom session- parameters. Do not toggle between both.

- CSCts12193

  Symptoms: With the single hop MPLS TE tunnel from the core router to the PE router, removing the MDT default configuration may cause some control planes to go down (like LDP, BGP). This is due to misprogrammed adjacency in the hardware.

  Conditions: This symptom occurs when unconfiguring the MDT default configuration.

  Workaround: Restore the configuration.

- 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.

- CSCts13720

  Symptoms: When static pseudowires are configured with VCCV BFD, some of the VCs may not come up.

  Conditions: This symptom occurs when a static pseudowire is configured with VCCV BFD.

  Workaround: For the VCs that are DOWN, issue the **clear xconnect peer** *peer-ip-address* **vcid** *vcid value* command to bring the VC back UP.

- CSCts14799

  Symptoms: Memory leak is observed on IPSEC key engine and IPSec background.

  Conditions: This symptom occurs with 2000 IPv6 over IPv4 GRE tunnels protected by IPSEC.

  Workaround: There is no workaround.

- CSCts15034

  Symptoms: A crash is seen at dhcpd_forward_request.

  Conditions: This symptom is observed with the DHCP relay feature when it is used with a scaled configuration and significant number of DHCP relay bindings.

  Workaround: If possible, from a functional point of view, remove the **ip dhcp relay information option vpn** command. Otherwise, there is no workaround.

- CSCts16013

  Symptoms: Longevity testing session churn causes RP crash on the Cisco ASR1K router. RP crash occurs due to memory leak by the QOS Accounting feature.

  Conditions: This symptom is observed during testing with the QOS Accounting feature PAC2. This issue is seen when there are a large number of sessions and churns with “aaa-accounting” in the QOS policy-map.

  Workaround: There is no workaround.

- CSCts16285

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

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

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

- CSCts18404

  Symptoms: A Flex VPN (IKEv2) client may lose complete connectivity via its VPNs even though SAs are in place.

  Crypto routes are missing, and the tunnel negotiated address is missing too. Other config-exchange information may be missing too.

  Conditions: This symptom is observed on a Flex VPN client that may end up having duplicate IKEv2 SAs with a server. When this condition occurs and one of the duplicate SAs is removed (which usually happens naturally but can also happen administratively), all config-exchange configurations are withdrawn despite the fact there is still another IKEv2 SA active.

  Workaround: There is no clean workaround.

  The only solution is to manually clear the IKEv2 SAs on the Flex Client to force a renegotiation. Because the Flex Clients can be disseminated in the field and because network conditions can trigger duplicate SAs on a massive amount of clients, this workaround is barely practical.

- CSCts20246

  Symptoms: The DR for the receiver segment forwards IPv6 multicast packets on the Accepting Interface of S,G.

  Conditions: This symptom occurs while multicast stream is running and the RPF interface towards the source and RP goes down on the DR and the interface connected to the receiver (oif in S,G before interface goes down) becomes the RPF interface for the source and RP and hence iif for S,G.

  Workaround: There is no workaround.

- CSCts23708

  Symptoms: No NHRP routes will be added for all other discovered prefixes.

  Conditions: This symptom is seen when spoke to spoke traffic is triggered.

  Workaround: There is no workaround.

- CSCts23841

  Symptoms: V-cookie is not present in account profile query replies.

  Conditions: This symptom is observed in recent ISG images.

  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.

- CSCts24348

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

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

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

- CSCts27042

  Symptoms: PIM bidirectional traffic loops upon DF-election and RPF-change.

  Conditions: The symptom is observed with several hundred streams combined with a routing change (interface shutdown/no shutdown or metric increment/decrement).

  Workaround: There is no workaround.

- CSCts27333

  Symptoms: Multicast traffic is forwarded in software due to MTU failures.

  Conditions: This symptom is seen with packet size greater than the standard interface MTU being forwarded on the standby supervisor in a VSS setup. The problem is only seen with GRE tunnel OIF, where the tunnel MTU is incorrect in spite of the underlying interface being configured to accept a higher MTU.

  Workaround: There is no workaround.

- CSCts28315

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

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

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

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

  Workaround: There is no workaround.

- CSCts31111

  Symptoms: Coredump generation fails on the Cisco 800.

  Conditions: This symptom occurs when coredump is configured.

  Workaround: Go to ROMmon, and set a variable WATCHDOG_DISABLE before the coredump happens, as follows:

  conf t config-reg 0x0 end wr reload yes <rommon prompt> DISABLE_WATCHDOG=yes sync set conf-reg 0x2102 reset

- CSCts31791

  Symptoms: Traceback is seen at id_to_ptr.

  Conditions: This symptom occurs when a multilink is brought up using a virtual-access in the Cisco 7600 or ASR platform.

  Workaround: There is no workaround.

- CSCts31868

  Symptoms: The router crashes at fmanrp_ess_is_valid_ess_segment.

  Conditions: This symptom is observed at fmanrp_ess_is_valid_ess_segment.

  Workaround: There is no workaround.

- CSCts31870

  Symptoms: Routed multicast traffic on Cisco ME 3600X and Cisco ME 3800X may be dropped intermittently.

  Conditions: This issue has been seen under the following conditions:

  – Cisco ME 3600X is running Cisco IOS Release 15.1(2)EY.
  – Multicast stream can be received on any type of interface (L2/L3).

  Packets are intermittently software switched and may be dropped on the CPU. Issue can be verified via the following:

```
Switch#show ip mfib 239.1.1.1
<output omitted>


 (*,239.1.1.1) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   332/0/1366/0, Other: NA/NA/NA
   Vlan100 Flags: A NS
   Vlan200 Flags: F NS
     Pkts: 0/0
 (10.0.0.10,239.1.1.1) Flags: HW
   SW Forwarding: 335/0/1344/2, Other: 0/0/0  <----  SW Forwarding for S,G
increments
   HW Forwarding:   16651904/778/1366/8305, Other: NA/NA/NA
   Vlan100 Flags: A
   Vlan200 Flags: F NS
     Pkts: 0/335
```

  Workaround: There is no workaround.

- CSCts32920

  Symptoms: Traffic gets punted to the RP.

  Conditions: This symptom occurs when there are multiple P2P-GRE tunnels in a particular VRF. Remove one particular P2P-GRE tunnel from that VRF.

  Workaround: Shut/no shut P2P-GRE tunnels in that particular VRF, for which traffic is getting punted to the RP.

- CSCts32963

  Symptoms: Standby is not coming up.

  Conditions: This symptom occurs when a distribute-list is configured. The ACL is created if it does not exist. Then remove the ACL, but the distribute-list configuration that ties to the ACL is not removed. Configure the IPv6 ACL configuration with the same ACL name. Save the configuration and reload it.

  Workaround:

1) When an access list is removed, remove corresponding distribute-list configuration as well.

2) Do not use the same access list name for IPv4 and IPv6.

- CSCts34693

  Symptoms: A Cisco router may crash with the following error message:

  000199: *Aug 23 16:49:32 GMT: %BGP-5-ADJCHANGE: neighbor x.x.x.x Up

  Exception to IOS Thread: Frame pointer 0x30CF1428, PC = 0x148FDF84

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = EEM ED Syslog -Traceback= 1#07279b80de945124c720ef5414c32a90 :10000000+48FDF84 :10000000+48FE400 :10000000+4B819C8 :10000000+4B81964 :10000000+F5FAD8 :10000000+F5FD10 :10000000+F5FEF0 :10000000+F5FF94 :10000000+F60608

  Conditions: This symptom is observed in a Cisco ASR 1004 router running IOS Release 15.0(1)S. This problem appears to be related to an EEM script that executes on a syslog event.

  event manager applet BGP-MON event tag BGP-DOWN syslog pattern "BGP-5-ADJCHANGE.*Down" event tag BGP-UP syslog pattern "BGP-5-ADJCHANGE.*Up" trigger correlate event BGP-DOWN or event BGP-UP action 02 cli command "enable" action 03 cli command "sh log" action 04 mail server "$_email_server" to "$_email_to" from "$_info_routername@mcen.usmc.mil" subject "Problems on $_info_routername, BGP neighbor Change" body "$_cli_result"

  Workaround: There is no workaround at this time.

- CSCts37314

  Symptoms: The session goes down after changing the BFD timers.

  Conditions: This symptom is observed after changing the BFD timers.

  Workaround: Perform shut/no shut on the interface.

- CSCts37446

  Symptoms: Traceback is observed while testing the antireplay feature.

  Conditions: Traceback is observed while configuring the routers randomly. It is not observed manually.

  Workaround: There is no workaround.

- CSCts39240

  Symptoms: The **advertise** command is not available in BGP peer-policy templates.

  Conditions: This symptom is observed on Cisco router running Cisco IOS Release 15.2(01.05)T, Cisco IOS Release 15.2(00.16)S, Cisco IOS Release 15.1 (03)S0.3, or later releases.

  Workaround: The keyword and functionality is still available to be configured in the BGP neighbor command.

- CSCts39284

  Symptoms: Packet is corrupted. The bottom of the label stack bit is not set correctly.

  Conditions: This symptom is seen when ibgp+label is configured.

  Workaround: There is no workaround.

- CSCts39535

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

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

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

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

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

- CSCts41217

  Symptoms: Memory leak occurs in const_mfib_lc_* processes.

  Conditions: This symptom is observed during deletion and addition of VRFs. Multicast needs to be enabled in the VRF and the P2P tunnels should be present in the VRF. VRF should be removed before deleting the P2P tunnels for this to happen.

  Workaround: Delete all the P2P tunnels before removing the VRF

- CSCts42154

  Symptoms: After the Cisco IOS ASR 1006 router is reloaded, it fails to reregister to the key server. From the debugs, it is observed that the attempt to register is generated too early before the GDOI is ON. This registration attempt is made before the interface, through which GDOI registration traffic with the key server passes, goes to the UP state.

  Conditions: This symptom is observed on a Cisco IOS ASR 1006 router that runs Cisco IOS Release 15.0(1)S2 and Cisco IOS Release 15.0(1)S3.

  Workaround: Use the **clear crypto gdoi** command to fix this issue.

- CSCts44718

  Symptoms: A router may crash.

  Conditions: The crash may occur when a service policy that has a flow monitor as an action is applied to a virtual interface and that virtual interface is deleted. It may also occur when the service policy is applied to a physical interface that is removed by OIR.

  Workaround: Before deleting (or OIRing) the interface, remove the flow monitor from the policy or the policy from the interface.

- CSCts45619

  Symptoms: T.38 Fax calls through the CUBE enterprise on the Cisco ASR platform with the Cisco IOS MTP colocated on the ASR can fail with cause 47 and subsequently leak a structure on the forwarding plane, causing future call failures.

  Conditions: This symptom is observed with T.38 calls through the CUBE enterprise on the Cisco ASR platform (only) with colocated MTPs in the call flow.

Workaround: On nonredundant ASR platforms, a reload is required to clear the hung structures on the forwarding plane. On the Cisco ASR1006 with redundant RPs and ESPs, you can perform a switchover of the ESPs (FPs) to clear the problem, as follows:

hw-module slot F0 reload ! confirm via show platform that the F0 is in a ok, standby state, takes some time for the F0 to reload. sh platform ! do not execute the below command until F0 is back online hw-module slot F1 reload ! again, confirm via show platform that the F1 is in a ok, standby state sh platform

- CSCts47566

  Symptoms: During standby RP bootup, an incorrect ICMP punt entry for MPLS interfaces gets programmed. This entry appears even if the interface has no ACL applied in the input/output direction.

  2037#show tcam inter gi4/0/3 acl in ip

  * Global Defaults shared

  Entries from Bank 0

  punt icmp any any eq 11 <<<<<<<<<<<<<<<< permit ip any any (1895 matches)

  Entries from Bank 1

  Conditions: This symptom is observed with the ICMP punt entry, which is required to allow trace route across MPLS cloud. This is a workaround for a hardware problem with Tycho. The feature is called “FM_FEATURE_MPLS_ICMP_BRIDGE”. This workaround is required only if there are aggregate labels programmed in the superman VPN cam, but can get set incorrectly even when there is no VRF configuration on the box.

  Workaround: To clear the entry set unnecessarily, disable/enable MPLS on the interface for which it appears.

- CSCts47605

  Symptoms: For ECMP on the Cisco ASR1k router, RSVP does not select the right outgoing interface.

  Conditions: This symptom is observed with RSVP configuration with ECMP.

  Workaround: There is no workaround.

- CSCts47776

  Symptoms: Router crashes due to Mediatrace performance monitor debug.

  Conditions: The issue is seen with debug performance monitor database.

  Workaround: There is no workaround.

- CSCts47982

  Symptoms: Multicast traffic drops on trunk ports with output drops incrementing.

  Conditions: This symptom is observed when non-rpf packets make it to the node due to the network redundancy. The hardware met is wrongly programmed for rpf- fail packet handling.

  Workaround: Shut the interface on which non-rpf packets are coming on. Alternatively, change the DR priorities so that multicast forwarding happens only from one of the nodes.

- CSCts48300

  Symptoms: Interface queue wedge may occur when malformed traffic is received on port UDP 465. A maximum of 50 packets will become wedged.

  Conditions: Some malformed traffic must exist.

Workaround: There is no workaround.

- CSCts49032

  Symptoms: Data traffic is getting block-holed.

  Conditions: This symptom occurs with the removal/addition of default MDT address in VRF, with time gap of 30 minutes.

  Workaround: Deletion/addition of VRF.

- CSCts51980

  Symptoms: STM1-SMI PAs of version 3.0 do not come up.

  Conditions: This symptom is observed when the new version of PAs do not come up with enhanced flexwan.

  Workaround: There is no workaround. Without the PA, flexwan will come up.

- CSCts52643

  Symptoms: Session will not get offloaded to hardware when enabling HWO using the **no platform bfd enable-offload** command.

  Conditions: This symptom is seen when all workload credit is allocated so no more sessions are coming up.

  Workaround: There is no workaround.

- CSCts55322

  Symptoms: More traffic is sent out because of stale MET entries.

  Conditions: This symptom occurs in a scale condition when the route towards the core on the source PE is changed.

  Workaround: There is no workaround.

- CSCts55371

  Symptoms: OSPF will not flood link state updates over an interface. The command **show ip ospf flood-list** will show interface entries similar to:

  Interface Tunnel1, Queue length 181 Link state retransmission due in 1706165974 msec

  Note the high value for the retransmission timer.

  Conditions: The symptom is observed with some newer S and T releases including Cisco IOS Release 15.1(2)S, Release 15.1(3)S, and Release 15.2(1)T.

  The issue can occur on interfaces where OSPF has not flooded updates for more than 24 days. This can include interfaces that are newly configured for OSPF if the router has been up longer than that. Interfaces that flood LSAs at least once every 24 days will not be affected.

  Workaround: To clear a hung interface use **clear ip ospf process**.

- CSCts56044

  Symptoms: A Cisco router crashes while executing a complex command. For example:

  show flow monitor *access_v4_in cache aggregate ipv4 precedence sort highest ipv4 precedence top 1000*

  Conditions: This symptom is observed while executing **show flow monitor** *top* top-talkers command.

  Workaround: Do not execute complex flow monitor top-talker commands.

- CSCts56277

  Symptoms: The Cisco IOSd crashes.

  Conditions: This symptom occurs during CC reload.

  Workaround: This issue is inconsistently seen. After the crash happens, the SIP comes up fine.

- CSCts57115

  Symptoms: After the following procedure is executed, multicast traffic on several VRFs is not forwarded to the outbound tunnel interface for MDT.

  The procedure is as follows: 1) Reload the router. 2) Perform RP switchover. 3) Perform active ESP(F0) hardware reload. 4) Perform active ESP(F1) hardware reload.

  Conditions: This symptom is observed when MVPN sends out multicast traffic on a lot of VRFs.

  Workaround: Use the **ip pim sparse-mode** command to reconfigure the loopback0(global) interface.

- CSCts57295

  Symptoms: The following commands will be displayed by the **show running configuration** command even if only the **mac- address-table notification change mac-address-table notification mac- move** command is used or if only the **mac address-table notification change mac address-table notification mac-move** command is used. Also, we can delete all of them by deleting one pair of them.

  mac-address-table notification change mac-address-table notification mac-move

  mac address-table notification change mac address-table notification mac-move

  When reloading the device with the above command, the switch crashes and reboots itself.

  Conditions: This symptom is seen when reloading the device with the following commands:

  mac-address-table notification change mac-address-table notification mac-move

  mac address-table notification change mac address-table notification mac-move

  Workaround: There is no workaround.

- CSCts58394

  Symptoms: The SNMP graph traffic rate (collected from the port-channel subinterface) does not match the 5-minute offered rate from “show policy-map inter port-channel x.x”.

  Conditions: This symptom occurs on the Cisco 7600-S running Cisco IOS Release 15.0(1)S4 with the port-channel subinterface on 76-ES+XC-40G3CXL. This issue is seen only when there is EARL recirculation of packets and affects only the ingress traffic rate.

  Workaround: There is no workaround.

- CSCts59014

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

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

  Workaround: There is no workaround.

- 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.

- CSCts62082

  Symptoms: Router generates the following message:

  %NHRP-3-QOS_POLICY_APPLY_FAILED: Failed to apply QoS policy 10M-shape mapped to NHRP group xx on interface Tunnelxx, to tunnel x.x.x.x due to policy installation failure

  Conditions: The symptom is observed when “per-tunnel” QoS is applied and there are more than nine DMVPN spokes. (Up to eight spokes, with QoS applied is fine.)

  Workaround: There is no workaround.

- CSCts63501

  Symptoms: The non-EOS forwarding path for the explicit null label (reserved label 0) is programmed as drop on the line card, resulting in PW traffic loss with an MPLS LDP explicit-null configuration.

  Conditions: The PW traffic loss occurs on line cards in which MPLS LDP explicit-null is set.

  Workaround: There is no workaround.

- CSCts64539

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

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

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

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

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

- 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).

- 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.

- CSCts68541

  Symptoms: In IPsec scaling test, when CPE is keeping reload, all IPsec sessions will be torn down and reestablished. During the session flapping, RP reset is observed sometimes.

  Conditions: This symptom is seen with CPE reloading continually.

  Workaround: There is no workaround.

- CSCts68630

  Symptoms: IPv6 ACL may not match the traffic as per the configuration when there is an ACL configuration change.

  Conditions: This issue is seen when you configure an ACL list with a mix of ACL entries with the source address set to “any” and set with a specific value.

  Workaround: You can enter the ACL list entries in sequence in increasing order, for example:

  permit icmp any host 2A00:2180:400:212:31:220:174:1 sequence 10 permit icmp any host 2A00:2180:4400:204:109:193:249:1 sequence 20 permit icmp any host 2A00:2180:4400:192:199:150:1:1 sequence 30 log-input permit tcp any eq bgp host 2A00:2180:4400:204:109:193:249:1 sequence 110 permit tcp any host 2A00:2180:4400:204:109:193:249:1 eq bgp sequence 115 permit tcp any eq bgp host 2A00:2180:4400:192:199:150:1:1 sequence 120 permit tcp any host 2A00:2180:4400:192:199:150:1:1 eq bgp sequence 125 permit udp any eq 1645 any range 1024 49151 sequence 210 permit udp any eq 1812 any range 1024 49151 sequence 220 permit udp any eq bootps any eq bootps sequence 310 permit udp any host 2A00:2180:4400:204:109:193:249:1 range 3784 3785 sequence 410 deny ipv6 any 2A00:2180::/37 sequence 510 deny ipv6 any host 2A00:2180:4400:204:109:193:249:1 sequence 610 deny ipv6 any host 2A00:2180:4400:192:199:150:1:1 sequence 615 log-input permit ipv6 any any sequence 999 log-input

- CSCts69204

  Symptoms: PPPoE sessions do not get recreated on the standby RP.

  Conditions: This symptom occurs on the standby RP.

  Workaround: There is no workaround.

- CSCts69973

  Symptoms: Spoke with 100 tunnels crashed at nhrp_process_delayed_resolution_event_wrapper.

  Conditions: Source interfaces of the tunnels started to bring up.

  Workaround: There is no workaround.

- 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.

- CSCts71958

  Symptoms: When the router is reloaded due to crash, the **show version** output shows the reload reason as below:

  Last reload reason: Critical software exception, check bootflash:crashinfo_RP_00_00_20110913-144633-PDT

  After this, the same reason is shown even if the router is reloaded several times using the **reload** command.

  Conditions: The issue seen after a crash.

Workaround: There is no workaround.

- 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.

- CSCts74982

  Symptoms: Performance Monitor is unable to create monitor object for policy because of collision when creating monitor object.

  Conditions: The issue is seen with dynamic Performance Monitor policy on Mediatrace routers.

  Workaround: There is no workaround.

- CSCts76410

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

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

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

- CSCts76964

  Symptoms: The Cisco ASR router crashes with tracebacks, as given below:

  Exception to IOS Thread: Frame pointer 0x7F5CED910380, PC = 0x2F4A2E7

  UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Crypto IKMP -Traceback= 1#261f9625131701783f9129d7afdd6633 :400000+2B4A2E7 :400000+4FAFFBF :400000+4F BC2FB :400000+4FBC662 :400000+371635B :400000+63E0B86 :400000+63DCB63 :400000+63F13A6 :400000+63F15 6D :400000+629144E :4 00000+63E51A1 :400000+64BE0B1 :400000+64BE037 :400000+63E5D59 :400000+624BB06 :400000+63DBC34

  Fastpath Thread backtrace: -Traceback= 1#261f9625131701783f9129d7afdd6633 c:7F5DE3D0F000+BDDD2

  Auxiliary Thread backtrace: -Traceback= 1#261f9625131701783f9129d7afdd6633 pthread:7F5DE1D0E000+A7C9

  RAX = 0000000000000000 RBX = 006DE6F05C7F0000 RCX = 0000000000000000 RDX = 0000000000000000 RSP = 00007F5CED910380 RBP = 00007F5CED9103A0 RSI = 0000000000000000 RDI = 4060D60A00000000 R8 = 00000000F0466060 R9 = A038E6F05C7F0000 R10 = 000000000AEF96B8 R11 = 8038E6F05C7F0000 R12 = 0000000000000000 R13 = 00007F5CF0A51A80 R14 = 4060D60A00000000 R15 = 0000000000000000 RFL = 0000000000010246 RIP = 0000000002F4A2E7 CS = 0033 FS = 0000 GS = 0000 ST0 = 0000 0000000000000000 ST1 = 0000 0000000000000000 ST2 = 0000 0000000000000000 ST3 = 0000 0000000000000000 ST4 = 0000 0000000000000000 ST5 = 0000 0000000000000000 ST6 = 0000 0000000000000000 ST7 = 0000 0000000000000000 X87CW = 037F X87SW = 0000 X87TG = 0000 X87OP = 0000 X87IP = 0000000000000000 X87DP = 0000000000000000 XMM0 = 0D0D0D0D0D0D0D0D0D0D0D0D0D0D0D0D XMM1 = 00040000000000000000080000040001 XMM2 = 806E29E230030000000000000000800 XMM3

= FD01000580030D028001000180010004 XMM4 = 00000000000000000000000000000000 XMM5 = 00000000000000000000000000000000 XMM6 = 00000000000000000000000000000000 XMM7 = 00000000000000000000000000000000 XMM8 = 00000000000000000000000000000000 XMM9 = 00000000000000000000000000000000 XMM10 = 00000000000000000000000000000000 XMM11 = 00000000000000000000000000000000 XMM12 = 00000000000000000000000000000000 XMM13 = 00000000000000000000000000000000 XMM14 = 00000000000000000000000000000000 XMM15 = 00000000000000000000000000000000 MXCSR = 00001F80

Writing crashinfo to bootflash:crashinfo_RP_00_00_20110308-100545-UTC

Conditions: The symptom is observed under the following conditions:

- GETVPN is operational on the Cisco ASR router.
- Registration to the Key-Server happens over the physical links.
- There is one primary and secondary link to the Key-Server.
- The crypto map is enabled on the primary interface first. Everything works fine here.
- The crypto map is enabled on the secondary interface.The ASR crashes as soon as you enable it on the Secondary interface with tracebacks, as shown above.
- The crash is also observed if the secondary interface is down and the crypto map is applied on it, although the crash is not observed instantly.
- The issue is also observed in Cisco IOS Release 15.1(3)Sa, along with Cisco IOS Release 12.2(33)XNE (could be reproduced only once at the first instance, and was not seen in subsequent tries) and Cisco IOS Release 12.2(33)XNF2.

When the same GDOI crypto-map is applied to two interfaces (in primary and secondary role), without the local-address configuration and TBAR enabled, and when KS sends the TBAR pseudotime update, the GM code gets confused between the two interfaces and the crash is observed. It is considered to be more of a timing issue.

Workaround 1: Disable TBAR on the Key-Server, that is, either with no replay or by changing it to counter-based to resolve the issue.

Workaround 2: Use the **crypto map** *name* **local-address** *logical-address* command globally on the Cisco ASR router and let the registration happen through the loopback.The loopback should be reachable to the Key-Server over the primary and the secondary links, respectively. Then, enable the crypto map on the primary and secondary interfaces, which will work fine.

- CSCts81427

  Symptoms: With a scaled dLFIoATM configuration on FlexWAN, after issuing SSO, some of the interfaces stop pinging.

  Conditions: This symptom is observed after doing SSO.

  Workaround: Shut/no shut of the ATM interface helps to resolve the problem.

- CSCts82058

  Symptoms: Creation of Overlay interface leads to router crash.

  Conditions: This symptom is seen when configuring overlay interface and enabling OTV commands followed by the **otv join-interface** command on the core facing interface.

  Workaround: There is no workaround.

- CSCts84357

  Symptoms: Router crashes when deconfiguring router ISIS which has the BFD enabled.

Conditions: This symptom is seen where there are multiple ISIS instances that have BFD enabled, and one of the ISIS instances is deleted.

Workaround: Do not enable ISIS BFD on multiple ISIS instances or disable ISIS BFD from the instance before deconfiguring it.

- 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.

- CSCts86788

  Symptoms: CPU Hog messages start to appear followed by a crash.

  Conditions: This symptom is observed when the **show mpls traffic-eng fast-reroute database interface** *name* **detail** command is issued on an interface where there are no MPLS-TE tunnels.

  Workaround: Do not issue this command on an interface where there are no MPLS-TE tunnels.

  Further Problem Description: The trigger is simple, that is, issuing the FRR **show display** command on an interface on which there are no MPLS-TE tunnels.

- CSCts88467

  Symptoms: Drops happen earlier than expected.

  Conditions: This symptom occurs if the queue-limit is incorrectly calculated.

  Workaround: Configure a queue-limit explicitly to fix this issue, then remove and reapply the policy. Configuring queue-limit in parent policy automatically triggers calculation based on the parent queue-limit value on the child queue-limits based on bandwidth allocated to various classes.

- 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.

- CSCts89761

  Symptoms:

  1. Inline service policy Configuration: Unable to configure monitor parameters once the flow monitor is specified. See the following example:

  Router(config)#interface GigabitEthernet0/2/1 Router(config-if)#service-policy type performance-monitor inline input Router(config-if-spolicy-inline)#match access-group 110 Router(config-if-spolicy-inline)#flow monitor FM_DEF_TCP <--- After this point, all configs will print out an error message Router(config-if-spolicy-inline)#monitor parameters <----- Not accepted Router(config-spolicy-inline-mparam)#interval duration 10 <-------- Not accepted Router(config-spolicy-inline-mparam)#history 5 <---------- Not accepted

  2. Non-inline service policy: Unable to change monitor parameters once the flow monitor is bound to a policy-map and attached to an interface. See the following example:

  If an attempt is made to change monitor parameters of an already attached policy as below, it will be rejected.

  UUT_451(config)#policy-map type performance-monitor VM_POLICY UUT_451(config-pmap)#class VM_CLASS UUT_451(config-pmap-c)#flow monitor VM_MONITOR UUT_451(config-pmap-c)#monitor parameters UUT_451(config-pmap-c-mparam)#history 6 <---------- Error message will show up if previous history value is different UUT_451(config-pmap-c-mparam)#interval duration 7 <----- Error message will show up if previous interval duration is different UUT_451(config-pmap-c-mparam)#react 102 mrv <-------- Error message will show up if this react was not configured before or if the subsequent command changes the threshold value of the already-configured react.

  Conditions:

  1. This symptom is seen when configuring an inline service policy for performance monitor on ASR platform.
  2. This symptom is seen when modifying monitor parameters of a non-inline service policy for performance monitor on a Cisco ASR platform.

  Workaround:

  1. To configure inline service policy, always specify all monitor parameters first and put the **flow monitor** *monitor name* command as the last command in the configuration.
  2. To change monitor parameters, remove the service-policy by using the **no service-policy** command, make your changes, and then reattach the service-policy.

  The above configuration restrictions do not apply if the enclosing policy-map is not attached to any interface. Also the changes do not apply if you specify an "empty" flow monitor, for example a flow monitor without an enclosing valid flow record.

- CSCts90734

  Symptoms: IKEA message trace entry memory leak is seen.

  Conditions: This symptom occurs when there is an IPsec session.

Workaround: There is no workaround.

- CSCts91603

  Symptoms: Higher rate is seen on the QoS policies attached on the L3 interface, which has multicast interest.

  Conditions: This symptom is seen when the non-rpf packets make way into the node due to wrong handling by the hardware met. The L3 interfaces see these packets where they are dropped. But before they get dropped, they get accounted in the egress QoS policy on the L3 interface.

  Workaround: Shut the interface on which these non-rpf packets make way or clear the multicast groups once.

- 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.

- CSCts97803

  Symptoms: When a policy-map is configured with two RTP class-maps and two RTP encapsulated MDI class-maps, flows are monitored on them. Changing one of the RTP class-maps to MDI will lead to the crash. Also when a policy-map is configured with both RTP and MDI class-maps, and if the flow being monitored by them is RTP encapsulated MDI flows, then RTP monitoring will not work.

  Conditions: This symptom is seen when policy-map is configured with both RTP and MDI class-maps. The RTP flow to be monitored should be RTP encapsulated MDI flow.

  Workaround: There is no workaround.

- 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.

- CSCts98336

  Symptoms: IKEv2 router crashes in exec when unconfiguring an active IKEv2 profile.

  Conditions: The symptom is observed when an IKEv2 profile is in use. The crash is occurring only if the profile is configured in a certain way.

  Workaround: Unconfigure first the AAA authorization block.

Conf t crypto ikev2 profile <profilename> no aaa authorization group <type> list <AAA list name> name-mangler <Mangler name>

no crypto ikev2 profile <profilename>

- CSCtt00253

  Symptoms: When both active and standby are Up, active crashes.

  Conditions: This symptom occurs when doing redundancy force switchover.

  Workaround: There is no workaround.

- 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.

- CSCtt03126

  Symptoms: Cisco ME 3600X is not passing multicast packets to 224.0.0.x through EVC configuration unicast traffic and multicast traffic except 224.0.0.x passes through without any issues. This has been observed on TenGig interface on the Cisco ME 3600X.

  Conditions: This symptom is seen under the following conditions:

  1. Bridge Domain is greater than 4094 or
  2. Spanning tree mode is not MST or
  3. Packets coming into the Cisco ME 3600X are untagged.

  Workaround:

  1. Make sure that the packets coming into the Cisco ME 3600X are tagged with VLAN ID. If it is a L3 port, then create a subinterface and configure encapsulation dot1q vlan.

2. Configure Spanning Tree mode as MST.
3. Bridge Domain should be less than 4094.

- CSCtt03485

  Symptoms: ES40: IDBMAN crash is seen with “no ip flow-export destination <> vrf <>”.

  Conditions: This symptom occurs when “ip flow-export destination 10.21.1.1 3000 vrf vrf_1120” is removed.

  PE2(config)#no ip flow-export destination 10.21.1.1 3000 vrf vrf_1120

  PE2#show vlan internal usage | i NDE both NDE internal VLANs 1013, 1015 are cleared from ’internal VLAN table’

  PE2#show monitor event-trace idbman all | i NDE clear NDE_1013 vlan 1013 clear NDE_1013 vlan 1013 mapping 1013 is cleared, but 1015 is not cleared from idbman mapping

  PE2#test platform debugger callfn name idbman_dump_vlans 0 Calling address (0x0AF46AFC) 1: Vl1 : 1 1015: NDE_1015 : 1015 mapping 1015 is still present in IDBMAN, eventhough 1015 is a free VLAN, so, it can be allocated to any new interface

  Now, 1015 can be allocated for any other new interface, as it is cleared from “internal VLAN table”, whereas it is not cleared from IDBMAN mapping. Thus, you can reproduce the IDBMAN inconsistency with NDE interfaces.

  When a new interface comes UP, the IDBMAN set will fail, as there is already an old mapping existing (NDE_1015). When you try to delete this new interface, it will try to clear the mapping in IDBMAN. But, it finds the old mapping (NDE_1015); hence, you must perform forced crash in idbman_if_clear_vlan_id and configure “ip flow-export destination 10.21.1.1 3000 vrf vrf_1120”.

  PE2#show vlan internal usage | i NDE 1013 NDE 1015 NDE_vrf_0

  PE2#show monitor event-trace idbman all | i NDE set NDE_1013 vlan 1013 set NDE_1015 vlan 1015

  PE2#test platform debugger callfn name idbman_dump_vlans 0 Calling address (0x0AF46AFC) 1: Vl1 : 1 1013: NDE_1013 : 1013 1015: NDE_1015 : 1015

  Workaround: Reload.

- CSCtt04093

  Symptoms: VC is not coming up after unshutting the preferred path/Tunnel.

  Conditions: This symptom is seen when configuring ATOM Tunnel from CE1 to CE2 using next hop destination address as preferred path and disabling fall back option.

  Shut down the preferred path and verify that AToM VC is not routed to another available route and that AToM VC is down.

  Now the preferred path is not found, and VC is down.

  Workaround: There is no workaround.

- CSCtt04411

  Symptoms: Load image on router with c7200-adventerprisek9-mz.152-1.12.T.

  Conditions: This symptom is observed when verifying the SNMP configurations on server for the entry of the threshold table.

  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.

- CSCtt07525

  Symptoms: Spoke router may crash when NHRP is cleared on another spoke.

  Conditions: The symptom is observed with FlexVPN and with spoke-to-spoke tunnels.

  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.

- CSCtt11748

  Symptoms: RP crashes when route-map is deleted.

  Conditions: This symptom occurs when removing route-map. The match and set <default> interface NULL0 causes the crash.

  Workaround: Remove match and set clauses before removing route-map.

- CSCtt12919

  Symptoms: Invalid queueing policy is accepted.

  Conditions: This symptom is seen when a flat queueing policy is accepted, which used to be valid for FRTS.

  Workaround: There is no workaround. The policy is invalid and will never be installed.

- CSCtt15963

  Symptoms:

  1. Inline service policy Configuration: Unable to configure monitor parameters once the flow monitor is specified. See the following example:

     Router(config)#interface GigabitEthernet0/2/1 Router(config-if)#service-policy type performance-monitor inline input Router(config-if-spolicy-inline)#match access-group 110 Router(config-if-spolicy-inline)#flow monitor FM_DEF_TCP <--- After this point, all configs will print out an error message Router(config-if-spolicy-inline)#monitor parameters <----- Not accepted Router(config-spolicy-inline-mparam)#interval duration 10 <-------- Not accepted Router(config-spolicy-inline-mparam)#history 5 <------------ Not accepted

  2. Non-inline service policy: Unable to change monitor parameters once the flow monitor is bound to a policy-map and attached to an interface. See the following example:

     If an attempt is made to change monitor parameters of an already attached policy as below, it will be rejected.

UUT_451(config)#policy-map type performance-monitor VM_POLICY
UUT_451(config-pmap)#class VM_CLASS UUT_451(config-pmap-c)#flow monitor
VM_MONITOR UUT_451(config-pmap-c)#monitor parameters
UUT_451(config-pmap-c-mparam)#history 6 <---------- Error message will show up if
previous history value is different UUT_451(config-pmap-c-mparam)#interval duration 7 <-----
Error message will show up if previous interval duration is different
UUT_451(config-pmap-c-mparam)#react 102 mrv <-------- Error message will show up if this
react was not configured before or if the subsequent command changes the threshold value of
the already-configured react.

Conditions:

1. This symptom is seen when configuring an inline service policy for performance monitor on ASR platform.
2. This symptom is seen when modifying monitor parameters of a non-inline service policy for performance monitor on a Cisco ASR platform.

Workaround:

1. To configure inline service policy, always specify all monitor parameters first and put the **flow monitor** *monitor name* command as the last command in the configuration.
2. To change monitor parameters, remove the service-policy by using the **no service-policy** command, make your changes, and then reattach the service-policy.

The above configuration restrictions do not apply if the enclosing policy-map is not attached to any interface. Also the changes do not apply if you specify an “empty” flow monitor, for example a flow monitor without an enclosing valid flow record.

- CSCtt16102

  Symptoms: Tracebacks are seen after unconfiguring ACL configuration.

  Conditions: This symptom is seen when configuring an ACL and removing the configuration. Tracebacks are observed on unconfiguring the ACL.

  spoke2(config)#ip access-list standard ha_rtr > spoke2(config-std-nacl)# permit 50.0.0.0 0.255.255.255 spoke2(config)# no ip access-list standard ha_rtr % The acl is not > configured.

  Workaround: There is no workaround.

- CSCtt16487

  Symptoms: High CPU is seen when changes are made to the Cisco WCCP Access Control List (ACL).

  Conditions: This symptom is observed in a Cisco WCCP ACL.

  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.

- 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.

- CSCtt18743

  Symptoms: On a Cisco IOS ISR G2 router with CUBE feature, intermittent registration fails in P2P mode registration pass-through.

  Conditions: This symptom occurs if the CallID in the “show sip-ua registration passthrough status” is larger than a certain value.

  Workaround: Reload the Cisco IOS ISR G2 CUBE router.

- CSCtt19442

  Symptoms: Cisco 7600 subinterface that is configured for bridging after router reload sends traffic even when being shutdown. This traffic is sent from physical interface to which subinterface correspond and further received on the other side of the link.

  Conditions: This symptom is seen when bridging is configured on subinterface.

  Workaround:

  - Doing a **no shutdown**, then **shutdown** on the subinterface clears the issue. - Remove bridging configuration from subinterface.

  Deleting subinterface, and then recreating it does not fix the issue.

- CSCtt23038

  Symptoms: IOSD crashes while executing the **show flow monitor name monitor2** command after an RP downgrade on bay 0.

  Conditions: This symptom is observed during a Cisco ASR 1004 ISSU downgrade from MCPDEV to Cisco IOS XE Release 3.5.

  Workaround: There is no workaround.

- CSCtt23367

  Symptoms: The status on active PoA is A/U. The status on standby PoA is S/A.

  Conditions: This symptom is seen after HA switchover. When configuring a new mLACP port-channel on new ACTIVE RP, it may get stuck in A/U state.

  Workaround: Remove the port-channel and RG configuration and add back again.

- CSCtt24777

  Symptoms: RP crashes at be_crypto_ipsec_update_peer_path_mtu.

  Conditions: This symptom occurs when configuring the tunnel MTU.

  Workaround: There is no workaround.

- CSCtt25612

  Symptoms: The router crashes with traceback error messages and the standby takes over. After this, the router is stable.

  Conditions: There is no known trigger or changes that were made as per the user update.

  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.

- 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.

- CSCtt26643

  Symptoms: A Cisco ASR 1006 router 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 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 his 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.

- 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.

- CSCtt30212

  Symptoms: IP SLA CFM Probes over PW fail.

  Conditions: This symptom occurs when ECMP exists towards the core.

  Workaround: Do not have ECMP.

- 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.

- CSCtt33158

  Symptoms: If WRED is already present and the queue limit is configured in packets then WRED thresholds become 0.

  Conditions: Use the below mentioned config to repro the problem.

  policy-map parent class class-default shape aver 2000 service-policy child

  policy-map child class class-default random-detect

  int g0/0/0 service-policy out parent

  policy-map child class class-default queue-limit 2000

  Workaround: Remove WRED and reattach it.

- 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

- CSCtt35936

  Symptoms: EIGRP route updates are not sent to DMVPN spokes. The **show ip eigrp inter** command output shows pending routes in interface Q, which remains constant. The **show ip eigrp int deta** command output shows that the next sequence number of the interface remains the same (does not advance).

  Conditions: This symptom occurs when EIGRP session flapped, resulting in routes being withdrawn and restored.

  Workaround: Add a static route on any spoke that kicks out EIGRP learned routes from the RIB table; this will again kick the interface on the HUB.

- CSCtt36513

  Symptoms: Crash seen on a Cisco ASR for the process IPSec key engine.

  Conditions: The symptom is observed when you have more than 4K sessions up on the ASR.

  Workaround: There is no workaround.

- CSCtt36757

  Symptoms: The following error message is noticed when configuring QoS on the interface of an ES+ card:

  %X40G_QOS-DFC9-3-CFN: qos tcam programming failed for policymap AGGR-CHA-INTERFACE-OUTPUT-POLICY

  Conditions: The symptom is observed after a misconfiguration in the interface. The interface was misconfigured as switchport which removed the QoS configuration from the interface configuration but not from the line card. After the interface was configured back to an L3 port, the issue started occurring when the same policy was reapplied.

  Workaround: A new policy can be applied but the required policy cannot be applied again.

- CSCtt37516

  Symptoms: Line card crash with priority traffic when QoS policy is applied.

  Conditions: The symptom is observed with the QoS priority feature.

  Workaround: There is no workaround.

- 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.

- CSCtt43552

  Symptoms: A Cisco router reloads with the **warm-reboot** command.

  Conditions: This symptom is observed on the Cisco router while running Cisco IOS Release 15.2(2.2)T.

  Workaround: There is no workaround. Remove CLI “warm-reboot” from configuration (router will not be able to use warm reboot feature)

- CSCtt43834

  Symptoms: Netflow counter gets incremented when sending SSM group range as v2.

  Conditions: The symptom is observed when doing an SSO.

Workaround: There is no workaround.

- 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.

- 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.

- CSCtt46730

  Symptoms: Platform crashes during IKEv2 negotiation between the spoke and the hub with Cisco TrustSec (CTS) enabled on the Cisco 3945E platform.

  Conditions: This symptom is seen with re-negotiation of IKEv2 SA between the peers.

  Workaround: There is no workaround.

- CSCtt46873

  Symptoms: In an MVPN setup, when the **mdt default** command is removed from under the VRF, unicast packets coming from the core, such as LDP and BGP, get dropped, leading to router isolation.

  Conditions: This issue is primarily seen when mls mpls tunnel-recir is not configured on the box (or does not get enabled due to the absence of a sip10g device). In such a case, MDT tunnel VLAN gets allocated, but is never released, until the **mdt default** command is removed. Since the decap adjacency handling the unicast packets is a GRE decap, with an MDT tunnel VLAN allocated, removal/re-add of **mdt default** command will program the adjacency with the MDT tunnel VLAN. Another removal along with a race condition might leave the adjacency with the tunnel VLAN (now deallocated), thereby causing the unicast packets to be dropped.

Workaround: Configure mls mpls tunnel-recir on the box and remove/re-add the **mdt default** command or reload with mls mpls tunnel-recir configured to be safe.

- CSCtt70585

  Symptoms: IPv6 traffic is not flowing.

  Conditions: This symptom is seen with IPSec v6 tunnels.

  Workaround: There is no workaround.

- CSCtt90672

  Symptoms: CFM MEP enters the INACTIVE state on deleting the subinterface.

  Conditions: This symptom is observed under the following conditions:

  1. Create a subinterface (vlan 104) for EOAM communication. Check “CC-Status” = Enabled.
  2. Create a QinQ subinterface (vlan tags: 104 128) for subscriber on the same physical interface. Check “CC-Status” = Enabled.
  3. Later, delete the QinQ subinterface from the step 2 above (DT’s provisioning system does it, for example, for a new policy change). The “CC-Status” goes to inactive.

  Workaround: Unconfigure and reconfigure the **continuity check** command under the corresponding Ethernet CFM domain/service global configuration for this CFM MEP.

- CSCtt98823

  Symptoms: Clock quality is bad from Cisco ME 3600X and Cisco ME 3800X.

  Conditions: This symptom is seen with normal network clock configurations.

  Workaround: There is no workaround.

- CSCtt99101

  Symptoms: Management port stops responding due to O/P queue wedge 40/40.

  Conditions: This issue is seen after 4-5 days when the box is up, and traffic is passing via management port.

  Workaround: Reload the box.

- 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.

- 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.

- CSCtu06894

  Symptoms: Cisco UBE crashes when the **show sip-ua calls** command is executed while there is an active SIP call through system.

  Conditions: This symptom is present on Cisco 2821 routers. The router crashes only when Cisco UBE receives an SDP length greater than 9000 bytes as part of a SIP message. And at the same time, if the show command is executed, the crash occurs. Otherwise, the crash is not seen.

  Workaround: There is no workaround.

- CSCtu07626

  Symptoms: Router processing SIP traffic crashes.

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

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

  Workaround: There is no workaround.

- 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.

- CSCtu11677

  Symptoms: A Cisco router may unexpectedly reload due to bus error or segV exception or generate a spurious error when the cSipStatsSuccessOkTable snmp object is polled.

  Conditions: This is seen on a voice gateway when the cSipStatsSuccessOkTable snmp object is polled.

  Workaround: Create an SNMP view and then block the oid for cSipStatsSuccessOkTable and then apply it to all SNMP communities on the device:

  snmp-server view blockmib iso include snmp-server view blockmib 1.3.6.1.4.1.9.9.152.1.2.2.5 exclude

  and then apply it to the community:

  snmp-server community <community> view blockmib ro

- 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.

- CSCtu13232

  Symptoms: Standby crash is observed on doing runversion between Cisco IOS Releases XE3.4.1 and XE3.6.

  Conditions: No special configurations are needed to reproduce.

  Workaround: There is no workaround.

- CSCtu14461

  Symptoms: Y.1731PM DMM probe cannot be successfully scheduled.

  Conditions: This symptom occurs on a Cisco ME 3800X platform. When a user schedules a Y.1731PM DMM probe on UP MEP with the core facing interface as switchport, statistics are not collected.

  Workaround: There is no workaround.

- CSCtu14878

  Symptoms: In unknown circumstances, when ECMP paths are created between a Cisco ME 3800 VPNv4 Pre-Agg router and a Cisco ASR 9000 3107 ABR router (through HA failures or intentional configuration), the ME 3800 will blackhole all VPNv4 traffic.

  Conditions: The symptom is observed with the following conditions:

  – Running IGP to 3107 ABR router.
  – Running labelled BGP to reach far end destination and to provide VPN labels.
  – Have ECMP paths from Cisco ME 3800 to Cisco ASR 9000 ABR router as shown from “show ip cef vrf vrfname prefix mask det”.

  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.

- 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.

- CSCtu18786

  Symptoms: Device may crash showing “VoIP” error messages. Decodes point to voice functions.

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

  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.

- CSCtu21967

  Symptoms: A router configured to be an IP voice gateway may crash.

  Conditions: The exact conditions for this crash are currently unknown.

  Workaround: There is no workaround.

- CSCtu22952

  Symptoms: Traffic stops forwarding suddenly when a port channel has an EVC configuration.

  Conditions: The symptom is observed when you have a port-channel interface with multiple member links on an LACP configured via EVC. By sending single source-destination traffic, it moves from one member link to another.

  Workarounds: Configure bridge-domain under the EVC and:

  1. Use etherchannel in FEC mode (mode ON) instead of LACP; or
  2. Remove EVC.

- CSCtu25150

  Symptoms: A Cisco router acting as a voice gateway may unexpectedly reload due to a SegV exception or bus error, or may experience a spurious access.

  Conditions: The exact conditions leading to the crash are not known. The issue is only present in Cisco IOS Release 15.1(4)M and later.

  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.

- 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.

- CSCtu29815

  Symptoms: If the CCM sub is restarted before the switchover from PUB to SUB, the MGCP GW needs at least 10 minutes to finish the switchover.

  Conditions: The symptom is observed under the following conditions:

  - MGCP GWx1. - Version: c2800nm-spservicesk9-mz.151-3.T.bin. - CUCM: version 8.6.1x2. - Primary CCMPUB and CCMSUB.

  Workaround: Restart the MGCP process from the gateway by using **no mgcp** and **mgcp**.

  Further Problem Description: When the CCMSUB's service is down (or machine is powered off), CM service sends a TCP FIN to MGCPGW, however from the debug of MGCPGW, the backhaul link between CCMSUB does not refresh as the TCP layer is stuck at CLOSEWAIT. It is confirmed that the MGCP GW is not notified about this at all, or the MGCP GW does not actively check the status the backup backhaul link.

  Then CCMSUB's started/powered on/recovered, however the CCMPUB is down/powered off this time. MGCP application itself will failover immediately, so does the backhaul link. However as the backhaul link's status was not updated as the TCP layer is still in CLOSEWAIT, the backhaul link is in a false OPEN status and CCM will not be able to leverage this gateway to make outbound calls and all incoming calls are being impacted as well.

- CSCtu30649

  Symptoms: Standby is reset.

  Conditions: This issue is seen when the ISSU standby is reset because of MCL failure.

  Workaround: There is no workaround.

- CSCtu31659

  Symptoms: Cisco ME-3600X series switch running Cisco IOS Release 12.2(52)EY2 and/or Release 15.1(2)EY will crash when the **diagnostic start test all** command is entered.

  Conditions: The symptom is observed with no specific configuration. The switch will crash with an empty configuration.

  Workaround: Avoid running the **diagnostic start test all** command.

- CSCtu32929

  Symptoms: DMVPN tunnel is failing to come up with Cisco TrustSec functionality enabled. NHRP is failing.

  Conditions: The symptom is observed when IKEv2 security association is up and NHRP negotiation fails to bring up the DMVPN tunnel.

  Workaround: Disable TrustSec CLI (with **crypto ikev2 cts sgt**).

- 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.

- CSCtu34207

  Symptoms: CoA for SessProv request timeout from ISG to SCE.

  Conditions: Issue is seen after an upgrade to Cisco IOS 15.1S train (seen in Cisco IOS Release 15.1(2)S1 too).

  Workaround: There is no workaround.

  Further Problem Description: The packet is seen in the TCPDUMP on the SCE. Cisco IOS Release 12.2(33)XNF2 does not show the issue. SCE shows in the debug:

  bad authentication validate failed

- 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.

- 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*.

- CSCtu35933

  Symptoms: L2 multicast groups stop being forwarded across EVC with IGMP snooping enabled.

  Conditions: The symptom is observed with a lot of IGMP activity. It occurs after a long time.

  Workaround: There is no workaround.

- CSCtu36562

  Symptoms: cikeFailureReason and cipsecFailureReason from CISCO-IPSEC-FLOW- MONITOR MIB do not report the proper failure reasons for failed IKE negotiations (ph1 or ph2).

  Conditions: The symptom is observed with failed IKE negotiations (ph1 or ph2).

  Workaround: There is no workaround.

- 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.

- 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.

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

  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.

- CSCtu51904

  Symptoms: You can observe decrementing free memory by each repetition of the process by using the **show memory statistics** command under the active SP.

  Conditions: The symptom is observed by removing "default mdt" under the VRF configuration and then adding it back. The memory leak is recognized on the active SP.

  Workaround: Reload the router.

- 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.

- 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.

- CSCtv21900

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

  Conditions: This symptom is observed under the following conditions:

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

  Phone logs show the following message:

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

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

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

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

- 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:

  Nov 10 08:09:00.238: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Up Nov 10 08:10:20.944: %BGP-3-NOTIFICATION: received from neighbor *X.X.X.X (hold time expired) x bytes Nov 10 08:10:20.944: %BGP-5-ADJCHANGE: neighbor *X.X.X.X Down BGP Notification received Nov 10 08:10:20.945: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from session Neighbor deleted Nov 10 08:10:34.328: %BGP_SESSION-5-ADJCHANGE: neighbor *X.X.X.X IPv4 Unicast topology base removed from session Neighbor deleted Nov 10 08:10:51.816: %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.

- 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 the IP/IPv6 addresses instead of the hostname for NTP configurations.

- 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.

- CSCtw50141

  Symptoms: Incremental leaks at __be_ber_get_stringa pointing to LDAP process.

  Conditions: The symptom is observed when NTLM authentication is being used with an LDAP server and with the router acting as the NTLM proxy.

  Workaround: There is no workaround.

- 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.

- CSCtw50941

  Symptoms: Crash occurs when trying to modify the class-map configuration of the SG aware firewall (using “match security-group”).

  Conditions: The symptom is observed with class-map configuration changes made on security-group class filters.

  Workaround: Do not attach the “match security-group” filter or modify the class-map with this filter.

- CSCtw51134

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

  Conditions: This symptom occurs after SSO.

Workaround: There is no workaround.

- CSCtw52097

  Symptoms: RG is stuck in STANDBY COLD-BULK state when the RG state is trying to restore to its appropriate state after a failover.

  Conditions: The symptom is observed when HA pairs are in an Active-Active scenario and control interfaces are using subinterfaces.

  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”.

- CSCtw53767

  Symptoms: ZBFW HA configured with A/R and QoS fails for asymmetric traffic.

  Conditions: The symptom is observed when ZBFW HA and QoS are configured together.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCtw60333

  Symptoms: HTTP process hangs. This impacts the webauth authentication scaling factor.

  Conditions: The symptom is observed when the **clear ldap server** *server-name* command issued or the connection is closed during any outstanding LDAP. Transactions are in progress or are waiting for an LDAP response from the LDAP server.

  Note: it is not only related to the secure-server. It is also applicable with an IP HTTP server. So generally it is applicable if you are using webauth with LDAP as the authentication server.

  Workaround: Do not issue **clear ldap server** when any LDAP transactions for web authentication are in progress.

- 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.

- CSCtw62858

  Symptoms: Cell payload scrambling is off by default for ATM DS1 interfaces on SPA-1CHOC3-CE-ATM.

  Conditions: The symptom is observed when you are using ATM or IMA DS1 T1 or E1 on any of these:

  - SPA-1CHOC3-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1). - SPA-2CHT3-CE-ATM (ATM DS3, ATM E3). - SPA-24CHT1-CE-ATM (ATM DS1, ATM E1, ATM IMA DS1, ATM IMA E1).

  Workaround: There is no workaround.

  Further Problem Description: Currently, cell payload scrambling is off by default for ATM DS1 interfaces on SPA-1CHOC3-CE-ATM and on for E1 interfaces. Cell payload scrambling is currently not configurable. This presents a problem when connecting to ATM copper T1 CPEs that require cell payload scrambling or when connecting to E1s devices that do not support cell payload scrambling.

- CSCtw66863

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

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

  Workaround: There is no workaround.

- 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.

- CSCtw72260

  Symptoms: Traffic flow is not learned.

  Conditions: The symptom is observed with a Cisco 7600 with line card and performance-traffic policy-map. Using IP-CBR, MDI, or RTP metric. Does not impact Cisco ASR 1000.

  Workaround: Do an OIR/reload.

- CSCtw72708

  Symptoms: Malloc failure, CPU hog, and memory leaks are seen creating the MD entry with your own IP address as the next-hop listener.

  Conditions: Issue is seen on a Cisco 7600 series router that is running Cisco IOS 15.2(04)S version. There are two triggers:

  1. When LI is configured on the Cisco 7600 with the remote's MDip as one of your own; resulting in CPU hog and memory failures.
  2. When one generic stream is deleted, an internal counter is decremented twice. Thus disabling the LI feature even when there is another active tap installed.

  Workaround: Configure the MD listener IP address with the correct IP address.

- CSCtw74099

  Symptoms: A Cisco ME 3600 may crash if the Ethernet Controller (eTSEC) tx ring is hung.

  Conditions: The symptom is observed if the management port is up.

  Workaround: Shut down the management port.

- CSCtw78064

  Symptoms: The **display-logout** message on a Cisco SCCP Phone is not cleared even after pressing other buttons on the phone.

  Conditions: This symptom is observed on the Cisco SCCP phone (also known as Skinny Phone or ePhone) when the last extension mobility (EM) user in a hunt group logs out using the HLog button. This symptom is observed even if the last EM user logs out of the hunt group and logs back in.

  Workaround: There is no workaround.

- CSCtw79488

  Symptoms: Multicast is not forwarded out on EVC.

  Conditions: This has been observed with Cisco IOS Release 15.1(2)EY and EY1a and with the following configuration:

  interface GigabitEthernetx/y switchport trunk allowed vlan none switchport mode trunk

  service instance <> ethernet encapsulation dot1q <VLAN-1> l2protocol tunnel bridge-domain <BD> ! !

  ! interface Vlan<BD> no ip address xconnect <IP> <VC-ID> encapsulation mpls !

  Workaround: Configure any dummy IP address on interface VLAN. It does not need to be in the same segment:

  ! interface Vlan<BD> ip address A.B.C.D M.M.M.M xconnect <IP> <VC-ID> encapsulation mpls !

- 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.

- CSCtw84414

  Symptoms: Standby reset due to configuration sync failure.

  Conditions: The symptom is observed with the CLI **monitor session** *session* **source remote vlan**.

  Workaround: There is no workaround.

- CSCtw84664

  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

- 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.

- CSCtw86212

  Symptoms: ISG is failing to support radius attribute filter configuration.

  Conditions: ISG is setting up a session via EAP/RP authentication, whereas authorization radius attribute(s) should be passed on by ISG to its radius client and ISG should ignore it locally when creating the session. It occurs only in the case of radius proxy.

  Workaround: Possibly do not send the undesired radius attributes to ISG in authentication/authorization replies and configure the required parameters on each radius-client (from an ISG perspective).

- CSCtw86712

  Symptoms: RP crashes.

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

  Workaround: There is no workaround.

- CSCtw86793

  Symptoms: A Cisco router running Cisco IOS 15.2T will generate phase II rekeys using IKEv1 instead IKEv2.

  Conditions: The symptom is observed with an IKEv2 DVTI hub (tunnel mode GRE IP).

  Workaround: Anchor the IKEv2 profile into the IPsec profile.

- CSCtw86880

  Symptoms: IOSD crashes during unconfiguration.

Conditions: The symptom is observed when you clear the IP sessions and then immediately unconfigure the port-bundle that is in use. Issue seems to be timing related.

Workaround: There is no workaround.

- CSCtw87783

  Symptoms: Applying a “match-protocol” causes the Cisco ASR 1000 to freeze and then reload.

  Conditions: This symptom appears when writing a “match-protocol ...” command while applying an MQC class-map on certain protocols (RTSP, NNTP).

  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.

- 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.

- CSCtw97513

  Symptoms: STP BPDUs are not sent over more than one VFI neighbor.

  Conditions: The symptom is observed with full mesh Virtual Private LAN Services (VPLS). The STP does not converge end-to-end.

  Workaround: There is no workaround.

- CSCtw98456

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

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

  For example, the IVRF routing table should show:

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

  but instead it shows:

S 10.0.0.0 [1/0] via 192.168.0.1

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

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

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

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

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

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

- CSCtw99290

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

  Conditions: 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.

- CSCtx00689

  Symptoms: Speed configurations may be rejected on standby. This causes a standby sync failure.

  Conditions: The symptom is observed when you configure speed on the main interface.

  Workaround: There is no workaround.

- CSCtx01329

  Symptoms: A Cisco 2921 using Cisco IOS Release 15.2(2)T and configured for crypto with access lists may have problems booting up. CPU hog messages and a watchdog crash may be seen.

  Conditions: The conditions are undetermined.

  Workaround: Use Cisco IOS Release 15.1(3)T.

- 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.

- CSCtx01918

  Symptoms: On the hub if you configure IVRF for static crypto-map then, after an invalid-spi recovery, the new ISAKMP has an incorrect IVRF (global). IPsec phase II fails with a “proxy identities not supported” error message. The other related issues seen are:

  1. Initial contact not being sent when IKE SA is triggered by invalid-spi recovery.

2. When quick mode is initiated, it picks the self-initiated IKE SA and hence the QM packet is dropped at the other end.

Conditions: The symptom is observed with a router running HSRP with VRF aware IPsec static crypto map. When you shutdown the active router's external interface, the IPsec tunnel failsover to the standby router. The standby router has an invalid-spi recovery configured. The invalid-spi recovery kicks but new ISAKMP has an incorrect IVRF and IPsec phase II fails.

Workaround: Manually clear SA at spoke site using **clear crypto sa**.

- CSCtx04712

  Symptoms: Removal of crypto map hangs the router.

  Conditions: The symptom is observed following removal of "gdoi crypto map" from interface.

  Workaround: There is no workaround.

- CSCtx05464

  Symptoms: CE multicast fails over VPLS when the PE device is an ME 3800x.

  Conditions: The symptom is observed with VPLS configured in a mesh with at least five VPLS peers.

  Workaround: For routing protocols, use unicast neighbors.

- 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.

- CSCtx16782

  Symptoms: FlexVPN hub to spoke stays in NEGOTIATING state.

  Conditions: The symptom is observed on a FlexVPN spoke and seen at connection with hub.

  Workaround: There is no workaround.

- CSCtx19332

  Symptoms: A Cisco router crashes when "remote mep" is unlearned while auto EOAM operations are executing.

Conditions: This symptom is observed if “remote mep” is unlearned from the auto database (shutdown on interface or remote mep reload) while the “IP SLA ethernet-monitor jitter” operation is still running. The crash occurs if the initial control message times out.

Workaround: There is no workaround.

- 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.

- CSCtx29557

  Symptoms: A standby crashes @ fib_fib_src_interface_sb_init.

  Conditions: All.

  Workaround: There is no workaround.

- 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.

- CSCtx34643

  Symptoms: MPLS pseudowire ping fails.

  Conditions: The symptom is observed when you configure MPLS with xconnect.

  Workaround: There is no workaround.

- 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.

- CSCtx41296

  Symptoms: When you do a **clear crypto session** in 4k flexVPN cases, the memory of crypto IKEv2 shows that it is increasing.

  Conditions: The symptom is observed with session flapping.

  Workaround: There is no workaround.

- CSCtx42722

  Symptoms: Routed multicast traffic is not forwarded out to all interfaces in OIL.

  Conditions: The issue seen on 15.1 code.

  Workaround: Issue a **clear ip mroute** *group* for the group in the broken state.

  Further Problem Description: The issue can be verified by checking **show platform ip multicast group** *group* **detail**. If encountering the issue, ports will be missing from the OIF for the S,G entry:

```
me3600x#sh platform ip multicast groups 224.0.10.135 detail
GROUP_ADDR 224.0.10.135

NMDB (*, 224.0.10.135) nmdb->0xD7E82E4, entry->0xE53D134 magic 0x9E tcam
hdl:0x277 nh_rpf_p:0xC3D85F8 nh_rpf_f:0xC3D8498 fid_hdl:0x13FD4D3C
(idx=0xBEB1) rpf pass:cpuQ:4 rpf falied cpuQ:5
 flags: HW, pflags: SPT,

RPF INTERFACE-> intf 501 port count (1) p10

RPF pass OIF interface count 1 hw_cnt 1
intf 224 port count 1 flags=0x8
 p11 <<<--- Correct port information getting reflected

RPF failed OIF interface count 1 hw_cnt 1 intf 224 port count 1 flags=0x8
 p11

GROUP_ADDR 224.0.10.135
```

```
NMDB (10.0.2.70, 224.0.10.135) nmdb->0xD7E64B4, entry->0xE53A494 magic 0xB6
tcam hdl:0x298 nh_rpf_p:0xC3DE4D8 nh_rpf_f:0x0 fid_hdl:0x13FDF8CC(idx=0xBEED)
rpf pass:cpuQ:0 rpf falied cpuQ:6
 flags: HW, pflags:

RPF INTERFACE-> intf 501 port count (1) p10

RPF pass OIF interface count 1 hw_cnt 1
intf 224 port count 0 flags=0x8
                                <<<<<---- Missing port information
```

- CSCtx44060

  Symptoms: Flexvpn spoke-to-spoke tunnels do not come up.

  Conditions: None.

  Workaround: Once tunnels fail to come up, clear the NHRP cache on one spoke alone.

- 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

- CSCtx49766

  Symptoms: GETVPN does not allow traffic in a Cisco HWIC-3G-CDMA-V modem.

  Conditions: This symptom is observed on a Cisco HWIC-3G-CDMA-V modem running Cisco IOS Release 15.1(4)M3.

  Workaround: Use Cisco IOS Release 15.1(3)T3 with the Cisco HWIC-3G-CDMA-V modem.

- 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

  show mpls traffic-eng link-management summary

  Workaround: There is no workaround.

- CSCtx54946

  Symptoms: CoA requests failing due to the error messages:

  CoA-NAK packet from host 10.10.10.14 port 1700, id=175, length=147 Reply-Message = "Push invoke failed Error-Cause = Unsupported-Service Cisco-Command-Code = "020;;turbo_button(in_p=3000000,out_s=3000000)" Cisco-Account-Info = "S18.0.23.175" Cisco-Account-Info = "$IVirtual-Access1.6017"

Conditions: The symptom is observed when you bring up 12K PTA sessions and send CoA request to all the sessions with VSA 252 0c attribute.

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.

- CSCtx57584

  Symptoms: SIP basic call fails with 500 internal server error.

  Conditions: The symptom is observed with Cisco IOS interim Release 15.2(02.14) T.

  Workaround: There is no workaround.

- 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.

- CSCtx62215

  Symptoms: In the presence of ingress and egress marking, ingress exp marking stops working.

  Conditions: The symptom is observed only when you reload the router in the presence of ingress and egress marking.

  Workaround: Detach and reattach the ingress policy which does exp marking.

- 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.

- CSCtx63545

  Symptoms: Box will crash in case of all the configured radius servers are dead and tried to authenticate client against RADIUS in the Radius-proxy case.

  Conditions: This will happen only for Radius-Proxy senario and if all the configured radius servers are dead.

  Workaround: Configure one of the alive RADIUS Servers.

- CSCtx63716

  Symptoms: Traceback seen @ cmfib_lc_process_entry.

  Conditions: There are no specific conditions.

  Workaround: There is no workaround.

- CSCtx66011

  A vulnerability in the Internet Key Exchange (IKE) protocol of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a device reload.

  The vulnerability is due to incorrect handling of malformed IKE packets by the affected software. An attacker could exploit this vulnerability by sending crafted IKE packets to a device configured with features that leverage IKE version 1 (IKEv1).

  Although IKEv1 is automatically enabled on a Cisco IOS Software and Cisco IOS XE Software when IKEv1 or IKE version 2 (IKEv2) is configured, the vulnerability can be triggered only by sending a malformed IKEv1 packet.

  In specific conditions, normal IKEv1 packets can also cause an affected release of Cisco IOS Software to leak memory.

  Only IKEv1 is affected by this vulnerability.

  An exploit could cause Cisco IOS Software not to release allocated memory, causing a memory leak. A sustained attack may result in a device reload.

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

  This advisory is available at the following link:

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

  Note: The September 25, 2013, Cisco IOS Software Security Advisory bundled publication includes eight Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2013 bundled publication.

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

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

- CSCtx67290

  Symptoms: A Cisco Session Border Controller crashes when receiving an oversize rtcp-fb element in the SDP.

  Conditions: The symptom is observed when there is an oversize rctp-fb element in the SDP.

  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”.

- CSCtx68100

  Symptoms: On a system having SP-RP, the reload reason is not displayed correctly. Once the system crashes, in all subsequent reloads the last reload reason is displayed as crash.

  Conditions: The symptom is observed on a system having SP-RP. The reload reason is shown wrongly when the **show version** CLI is executed.

  Workaround: There is no workaround.

- 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 Cisco ASR1001. IP options field includes “loose source routing” option.
  2. Cisco 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.

- CSCtx76780

  Symptoms: DHCP relay does not work on Cisco ME 3600.

  Conditions: This issue is observed if you configure at the same time a “ip helper-address” and an xconnect under the VLAN interface. It is observed on ME 3600/ME 3800 platforms running Cisco IOS Release 15.1(2)EY1 or earlier.

  Workaround: There is no workaround.

- CSCtx87939

  Symptoms: When the **Mediatrace Poll** command is invoked using WSMA interface, the “hops response received notifications” message is displayed. This message corrupts the WSMA output for the command.

  Conditions: This symptom is observed when Mediatrace poll is used in a WSMA interface.

  Workaround: There is no workaround.

- CSCtx89538

  Symptoms: The following error message may appear on a Cisco ME 3800 that is running Cisco IOS Release 15.1(2)EY1a when attaching ingress policy with marking to a service instance:

  Qos:Out of internal resources %QOSMGR-3-LABEL_EXHAUST: Internal Error in resource allocation

  Conditions: The symptom is observed with:

  - A Cisco ME 3800.
  - Cisco IOS Release 15.1(2)EY1a.

Workaround: There is no workaround.

- CSCtx90299

  Symptoms: The DMVPN IPsec sessions might get torn down and unable to re- establish themselves after experiencing link-flap events.

  Conditions: In a scaled DMVPN environment, when physical-port link-state up/down events happen, there will be stormed IPSec events to tear down and/or re-negotiate the sessions; it might run into a bad state that it cannot establish new sessions. Hence, when those active sessions expire (by time period or volume based), it can no longer be re-created. After some period of time, no more active session remains on the router.

  Workaround: Reload the router.

- CSCtx92665

  Symptoms: Executing the **show mediatrace session stat** command causes a crash at *__be_sla_mt_route_data_print*.

  Conditions: This symptom is observed when **show mediatrace session stat** or **show mediatrace session data** is used.

  Workaround: There is no workaround.

- 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.

- CSCty00734

  Symptoms: OSPF failing over xconnect between CE-CE connected via xconnect.

  Conditions: The symptom is observed with a change in L3 adjacency.

  Workaround: Use the following command: **clear xconnect** *peer vcid*.

- 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.

- CSCty04213

  Symptoms: “Max aces 1000” is configured for an ACL and attached to a interface. Unconfiguring either ACL or ACEs under the ACL leads to a system crash.

  Conditions: The symptom is observed when an ACL configured with 1000 ACEs is attached to interface for ingress or egress packet processing and later when either the ACL is configured or one of the ACEs is unconfigured in the ACL, you will see a crash of the Cisco ME 3600/ME 3800 device.

  Workaround: There is no workaround unless you can configure the number of ACEs less than 1000 per ACL.

- 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.

- CSCty12055

  Symptoms: A Cisco ASR 1000 6RU acting as IPsec-DMVPN hub with 4K sessions up on the router may unexpectedly reload at “IPSec background proc” within a few hours.

  Conditions: The symptom is observed on a Cisco ASR 1000 6RU acting as IPsec- DMVPN hub.

  Workaround: There is no workaround.

- CSCty15615

  Symptoms: Policy in direction A may disappear after removing policy from direction B. The policies no longer show up under the interface in **sh policy-map int** or **show running**.

  Conditions: The symptom is observed with policies on both input and output directions, and then you remove from one of the directions. Happens on Cisco 7200/7600 platforms.

  Workaround: There is no workaround.

- CSCty16623

  Symptoms: Traffic getting black holed because the VPN corresponding to the tunnel secondary VLAN gets programmed with punt adjacency.

  Conditions: The symptom is observed with unconfiguring-reconfiguring the VRF. (The issue is independent of time gap between the configuration change.)

  Workaround: There is no workaround.

- CSCty24707

  Symptoms: Standby RP continually reboots and never recovers.

  Conditions: The symptom is observed during an RP standby switchover with QoS applied to ISG sessions.

  Workaround: Shut down the virtual template interface and do a switchover.

- 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