Caveats in Cisco IOS XE 3.2S Releases

This chapter provides information about caveats in Cisco IOS XE 3.2S releases.

Because Cisco IOS XE 3S is based on Cisco IOS XE 2 inherited releases, some caveats that apply to Cisco IOS XE 2 releases also apply to Cisco IOS XE 3S. For a list of the software caveats that apply to Cisco IOS XE 2, see the "Caveats for Cisco IOS XE Release 2" section at the following location:

http://www.cisco.com/en/US/docs/ios/ios_xe/2/release/notes/rnasr21.html

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access field notices from the following location:

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

This chapter contains the following section:

Caveats in Cisco IOS XE 3.2S Releases

Caveats describe unexpected behavior. 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 chapter.

This section describes caveats in Cisco IOS XE 3.2S releases.

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

- Symptom—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/pcgi-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.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA)

This section consists of the following subsections:

Open Caveats—Cisco IOS XE Release 3.2.2S

This section documents unexpected behavior that might be seen in Cisco IOS XE Release 3.2.2S.

- CSCto32753

  Symptom: When the CES was reloaded or the **clear crypto session** command was run on the CES, existing IPSec SAs might not be automatically removed.

  Conditions: This issue was observed after the CES was reloaded or the **clear crypto session** command was run on the CES.

  Workaround: There is no workaround.

- CSCto52235

  Symptom: The **mac address accounting** command does not work.

  Conditions: There are no specific conditions under which this issue is observed.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS XE Release 3.2.2S

This section documents the issues that have been resolved in Cisco IOS XE Release 3.2.2S.

- CSCtn71898 and CSCto89992

  Symptom: During an ISSU subpackage upgrade from Release 3.2.x to Release 3.3.0, the router crashes. During an ISSU subpackage downgrade from Release 3.3.0 to Release 3.2.x, the standby RP does not come up correctly after the procedure. Instead, the standby RP reloads continuously and IPC timeout messages are generated each time the RP reloads.

  Conditions: These issues are observed when subpackage ISSU upgrade is performed on the router.

  Workaround: There is no workaround.

- CSCto81063

  Symptom: The IPv6 IPSec SVTI configuration does not work. The router reloads when you try to perform the configuration procedure.

  Conditions: This issue is observed when you try to configure IPv6 IPSec SVTI.

  Workaround: There is no workaround.

- CSCsl18054

Symptom: A local user created with a one-time keyword is automatically removed after failed login attempts. The expected behavior is that the one-time user should be removed after the first successful login, not after failed login attempts.

Conditions: This issue is observed on a router running Cisco IOS Release 12.4.

Workaround: There is no workaround.

- CSCta62394

  Symptom: The router reloads automatically when the standby RP tears down all IPSEC SAs.

  Conditions: This issue is observed on a router that is running SXF16 with IPSec High Availability and dynamic crypto maps configured on it.

  Workaround: Use static crypto maps instead of dynamic crypto maps.

- CSCth52252

  Symptom: If multiple EzVPN clients that are behind the same NAT device try to initiate sessions to the dVTI EzVPN server, when the first client connects to the server, traffic passes through the first client. However, when a second client connects to the server, traffic passes through the second client but fails on the first client.

  Conditions: This issue is observed when multiple EzVPN clients that are behind the same NAT device try to initiate sessions to the dVTI EzVPN server.

  Workaround: There is no workaround.

- CSCtj05903

  Symptom: When the router is reloaded, some virtual access interfaces are not created for the VT.

  Conditions: This issue is observed on scaled sessions.

  Workaround: There is no workaround.

- CSCtj20776

  Symptom: During authentication through CoA account login or TAL, a user profile with per-user configuration (such as idle-timeout, accounting, or QoS) is applied to the session. However, after all the actions have been performed, the per-user configuration is not installed and bound to the session.

  Conditions: This issue is observed during authentication in which a user profile containing per-user features is downloaded.

  Workaround: There is no workaround.

- CSCtj56142

  Symptom: In EAP reauthentication-related access requests, the user-name attribute provided may contain a dummy value, which is updated on session by ISG.

  Conditions: This issue is observed when EAP access requests carry a dummy user name during EAP reauthentication.

  Workaround: There is no workaround.

- CSCtj61748

  Symptom: At times, service activation fails.

  Conditions: This issue is observed when multiple services in the session authentication or authorization response are configured in the same service group.

  Workaround: Remove fields related to `service-group` and `service-type` from the service definitions.

- CSCtj79769

Symptom: The router crashes.

Conditions: This issue is observed when either IPv6 MLD snooping is disabled or IPv6 multicast itself is disabled.

Workaround: There is no workaround.

- CSCtj85333

  Symptom: The router may crash when the configuration template contains the **ip ips signature-category** configuration command and when the template is downloaded to the router by using the **cns config retrieve** command and the **cns config initial** command.

  Conditions: This issue is observed when the configuration commands mentioned in the Symptom description are used. This issue may also occur when the configuration template is downloaded to the router using the Config-Update operation of the configuration engine.

  Workaround: There is no workaround.

- CSCtj87846

  Symptom: The PfRtraffic class does not come out of the default state.

  Conditions: This issue is observed when a subinterface is used as an external interface and the corresponding physical interface shuts down and then restarts. The PfR master is not notified that the subinterface has restarted.

  Workaround: Shut down and then restart the PfR master or the PfR border.

- CSCtj94510

  Symptom: The router crashes at crypto_SS_process.

  Conditions: This issue is observed when all of the following conditions exist at the same time:

  - DMVPN is configured with more than 1000 tunnels.
  - There is one IKE session for each VRF.
  - There are four dual SAs per session.

  Workaround: There is no workaround.

- CSCtj99431

  Symptom: In a session, a shared key mismatch occurs between the ISG and the RADIUS client. However, the nonsubnet client (best match client) gets preference over the subnet client.

  Conditions: This issue is observed on a router that is used as an ISG RADIUS proxy router.

  Workaround: Remove the **ignore server key** setting from the **aaa server radius dynamic-author** configuration.

- CSCtk18607

  Symptom: The router crashes.

  Conditions: This issue is observed when **ip ssh pubkey** command is configured in both the user submode and the server submode.

  Workaround: There is no workaround.

- CSCtk31401

  Symptom: The router crashes when an SSH session is closed.

  Conditions: This issue is observed when **aaa authentication banner** command is configured on the router.

  Workaround: There is no workaround.

- CSCtk35953

  Symptom: Dampening information is not removed even when dampening is unconfigured in VPNv4 AF.

  Conditions: This issue is observed only if DUT has a eBGP-VPNv4 session with a peer and a same-RD import occurs on the DUT for the route learned from a VPNv4 peer.

  Workaround: Perform a hard reset of the session.

- CSCtk36582

  Symptom: Accounting On and Accounting Off messages from the AZR clear all the sessions in the client pool.

  Conditions: This issue is observed in any of the following scenarios:

  – When there are two AZRs, for example, 192.168.100.1 and 192.168.100.2, and you configure the client in the ISG under the RADIUS proxy as follows:

    ```
    client 192.168.0.0 255.255.0.0
    ```

  – The Accounting On or Accounting Off message from any of the clients clears sessions from both clients.

  Workaround: Configure the clients individually instead of configuring the client pool.

- CSCtk61069

  Symptom: The router crashes.

  Conditions: This issue is observed if you run the **priv exec level** *level* **show adjacency** command.

  Workaround: Do not set the privilege exec level for any form of the **show adjacency** command.

- CSCtk62950

  Symptom: Configuring SSH over IPv6 may cause the router to crash.

  Conditions: This issue is observed when SSH over IPv6 is configured.

  Workaround: There is no workaround.

- CSCtk67768

  Symptom: The RP crashes during the DHCPD receive process.

  Conditions: This issue is observed on a DHCP server that is used on a router acting as the ISG.

  Workaround: There is no workaround.

- CSCtk68109

  Symptom: The router reloads automatically when the CVP survivability.tcl script is run.

  Conditions: This issue is observed when **pass-thru content sdp** is used while configuring the router.

  Workaround: Use **codec transparent** instead of **pass-thru content sdp**.

- CSCtk74970

  Symptom: A tunnel that is announced by the TE autoroute is not installed in the routing table.

  Conditions: This issue is observed when you first configure and remove one hop and LDP from the TE, and then configure one hop on the TE (without LDP).

  Workaround: Run the **no ip routing protocol purge interface** command.

- CSCtl00770

  Symptom: The router stops responding during bootup.

  Conditions: This issue is observed when the following secure server WebUI configuration is used:

```
ip http secure-server
!
transport-map type persistent webui map-name
      secure-server
!
transport type persistent webui input map-name
```

Workaround: There is no workaround.

- CSCtl04285

  Symptom: After provisioning a new BGP session, a BGP route reflector may not advertise IPv4 MDT routes to PEs.

  Conditions: This issue is observed on a router running BGP, configured with a new-style IPv4 MDT, and peering with an old-style IPv4 MDT peer.

  Workaround: There is no workaround.

- CSCtl05684

  Symptom: XAUTH user information is displayed in the output of the **show crypto session summary** command.

  Conditions: This issue is observed when running EzVPN and, at the same time, performing XAUTH using a username that is different from the one used during P1 rekey.

  Workaround: To avoid sending a different username and password during P1 rekey, use the Save Password feature without enabling the interactive XAUTH mode.

- CSCtl21884

  Symptom: When enabling autosummary under the BGP process, a BGP withdraw update is not sent even when the static route goes down.

  Conditions: This issue is observed under any of the following conditions:

  - Autosummary is enabled under the BGP process.
  - A static route is brought into the BGP table by running the **network** command.

  Workaround: Use the **clear ip bgp *** command. Alternatively, disable the autosummary option under the BGP process.

- CSCtl50815

  Symptom: Prefixes remain uncontrolled. In addition, the following message is logged frequently without any actual routing changes:

  ```
  %OER_MC-5-NOTICE: Route changed Prefix <prefix> , BR x.x.x.x, i/f <if>, Reason
  Non-OER, OOP Reason <reason>
  ```

  Conditions: This issue is observed under the following conditions:

  - ECMP is used.
  - Mode monitor passive is configured.

  Workaround: Remove equal cost routing. For example, in a situation in which you use two default static routes, rewrite one of the two with a higher administrative distance and let PfR move traffic to that link as it sees fit. Alternatively, rewrite the two default routes and split them up in 2x /1 statics, one for each exit. This achieves initial load balancing. PfR balances the load correctly as required.

- CSCtl54033

Symptom: After the sub-LSP is pruned or torn down, resignaling sub-LSPs for P2MP TE tunnels may take up to 10 seconds.

Conditions: This issue is observed when a P2MP TE tunnel is configured to request FRR protection, but for the physical link down the path on the tunnel headend, there is no backup tunnel configured at the failure point (TE tunnel headend) to protect the sub-LSP. The TE tunnel headend takes up to 10 seconds to resignal the sub-LSPs.

Workaround: Configure FRR backup tunnels at the TE tunnel headend to provide link protection for P2MP TE tunnels for the physical link that is connected to the TE tunnel headend in the TE tunnel path.

- CSCtl54415

  Symptom: The router may reload.

  Conditions: This issue is observed when single-connection timeout is configured under an AAA group server and a TACACS key is not configured. For example:

  aaa group server tacacs name server-private x.x.x.x single-connection timeout 2 server-private x.x.x.x single-connection timeout 2 ip tacacs source-interface Loopback0

  Workaround: Ensure that you configure the correct matching key.

- CSCtl58005

  Symptom: When one of the following commands is run, an accounting start record is sent before an NCP has been negotiated:

  - **aaa accounting include auth-profile framed-ip-address**
  - **aaa accounting include auth-profile delegated-ipv6-prefix**
  - **aaa accounting include auth-profile framed-ipv6-prefix**

  Conditions: This issue is observed when **aaa accounting delay-start** is configured along with one of the commands listed in the Symptom description.

  Workaround: There is no workaround. If possible, avoid using the commands listed in the Symptom description.

- CSCtl67195

  Symptom: The following BGP debug commands do not run correctly:

  - **debug ip bgp vpnv4 unicast**
  - **debug ip bgp vpnv6 unicast**
  - **debug ip bgp ipv6 unicast**

  Conditions: This issue is observed when the BGP debug commands mentioned in the Symptom description are run.

  Workaround: There is no workaround.

- CSCtl83736

  Symptom: A V4 session setup leaks approximately 100 bytes. The following command can be used to verify the existence of this issue:

  show platform software memory messaging ios rp active | inc st_sb_cfg

  In the output of this command, the `diff` number increases continuously.

  Conditions: This issue is observed in IP sessions.

  Workaround: There is no workaround.

- CSCtl84797

  Symptom: SBC traceback occurs.

  Conditions: This issue is observed when LI is enabled and there are multiple media sessions in a single call (that is, SDP contains information about multiple media sessions).

  Workaround: There is no workaround.

- CSCtl88066

  Symptom: The router reloads automatically.

  Conditions: This issue is observed when BGP is configured and one of the following commands is run:

  - **show ip bgp all attr nexthop**
  - **show ip bgp all attr nexthop rib-filter**

  Workaround: Do not run either of these commands with the **all** keyword. Instead, run the address-family-specific version of the command for the address family.

- CSCtn01832

  Symptom: The following sequence of commands causes the router to crash at check syntax mode:

  1. **config check syntax route-map hello**
  2. **match local-preference**
  3. **no match local-preference**

  Conditions: This issue is observed when the sequence of commands mentioned in the Symptom description is run.

  Workaround: There is no workaround.

- CSCtn03930

  Symptom: System error messages are recorded in the router log.

  Conditions: This issue is observed on a router that functions as an IPSec termination and aggregation router. The issue occurs when RP switchover takes place while traffic is being processed.

  Workaround: There is no workaround.

- CSCtn07415

  Symptom: The router crashes at crypto_map_get_map_method_bitmask.

  Conditions: This issue is observed while reconfiguring IPSec with a large number (for example, 1300) of GRE tunnel interfaces while old configurations are present.

  Workaround: There is no workaround.

- CSCtn18784

  Symptom: Interface tunnel 0 sends constant high-bandwidth alarms.

  Conditions: There are no specific conditions under which this issue is observed.

  Workaround: There is no workaround.

- CSCtn22728

  Symptom: When running the **exi exi** command in the EVC mode, the standby RP may reload automatically due to configuration mismatch.

  Conditions: This issue is observed when the **exi exi** is run in the EVC mode.

  Workaround: There is no workaround.

- CSCtn24024

  Symptom: A router on which dynamic crypto maps are configured may experience a condition in which an IPSec SA decrypts traffic but does not encrypt traffic.

  Conditions: In general, this issue is observed when the remote peer IP address has changed. A duplicate flow is created in the hardware and, therefore, the traffic to be encrypted matches a stale flow.

  Workaround: Clearing the crypto session from the spoke might resolve the issue.

- CSCtn25100

  Symptom: PPP sessions take longer to start.

  Conditions: There are no specific conditions under which this issue is observed.

  Workaround: There is no workaround.

- CSCtn42916

  Symptom: In a redundant RP setup, when the active RP is physically removed from the chassis, the standby RP crashes.

  Conditions: This issue is observed on routers on which ASR1000-ESP40 is installed.

  Workaround: There is no workaround for this issue. Where possible, instead of performing a hardware OIR, perform an OIR by using the CLI.

- CSCtn53094

  Symptom: The router crashes or generates the following error message:

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

  Conditions: This issue is observed when alternating, with a very small delay, between the **ip pim** *mode* and **no ip pim** commands on an interface that is the only one on which PIM is enabled. The most common way this occurs in a production network is with the use of the **config replace** command, which results in the command alternating between ON and OFF and then to ON on a different interface.

  Workaround: There is no workaround. Avoid alternating between the **ip pim** *mode* and **no ip pim** commands on an interface that is the only one on which PIM is enabled.

- CSCtn56526

  Symptom: MBS is calculated on the basis of the MTU value. The user-defined MBS value is not displayed when the **sh atm pvc** command is run.

  Conditions: This issue is observed when a user-defined MBS value is set using the CLI.

  Workaround: There is no workaround.

- CSCtn59698

  Symptom: When an MLP bundle comes up on an LNS with conditional debugging based on the username that is enabled, certain attributes such as IDB description and IP-VRF are not applied on the MLP bundle virtual access interface.

  Conditions: This issue is observed when all the following conditions exist at the same time:

  - MLP sessions are configured on the LNS.
  - Per-user attributes, such as ip:vrf-id and ip:description, are configured in the user's RADIUS profile.
  - The session is started.

  - The **show interfaces** *Virtual-Access_intf* **configuration** command is run for both the member-link VA and the bundle VA.
  - The VRF and IDB descriptions sent by the RADIUS server is applied only on the member-link VA and not on the bundle VA.

  Workaround: Do not enable conditional debugs such as **debug condition username** *username*.

- CSCtn60353

  Symptom: When subpackage ISSU is performed, some OM objects on the standby RP may be missing.

  Conditions: This issue is observed when ISSU is performed across two releases and the target release adds a new TDL message type.

  Workaround: Force a reload of the standby RP before the final RP switchover.

- CSCtn64500

  Symptom: Multicast traffic does not pass through an ATM point to a multipoint sub-interface.

  Conditions: This issue is caused by an incomplete inject p2mp multicast adjacency on ATM P2MP interface. The output of the **show adjacency ATM interface detail** command shows that the `Inject p2mp Multicast` adjacency is in incomplete state.

  Workaround: Run the **clear adjacency** command to force repopulate the incomplete adjacency. Note that you should be aware of the impact of this system-wide command. As an alternative, use unicast commutation if it is possible to do so.

- CSCtn70367

  Symptom: The IPSec key engine crashes while sessions are being set up.

  Conditions: This issue is observed while setting up sessions with the configuration of 1000 VRFs, 1 IKE session per VRF, and 4 IPSec SA dual per session. The crash occurs while UUT is establishing the requested SAs.

  Workaround: There is no workaround.

- CSCtn73941

  Symptom: After performing an OIR for an ES+ card having EVC configuration with the **module clear-config** command enabled, reapplying the previous configuration does not work. In other words, traffic is not forwarded over the service instances. Even after changing the service instance numbers, the VLANs used in the previous configuration cannot be used effectively on the ports.

  Conditions: This issue is observed when **module clear-config** is configured.

  Workaround: There is no workaround.

- CSCtn81231

  Symptom: Multicast traffic is not forwarded from the RBE interface because the multicast adjacency is incomplete.

  Conditions: This issue is observed when the ATM DCHP host running IGMPv2 is established over an RBE interface to the router. The mutlicast group join is successful. However, the multicast adjacency is incomplete and it cannot forward multicast traffic.

  Workaround: Shut down and then restart the ATM main interface.

- CSCto03123

  Symptoms:

  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.

  Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.

  Workaround: There is no workaround.

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

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

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

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

- CSCto08790

  Symptom: When BRAS applies an ANCP shaper with a specific policy map name, ActualDownstreamRate, and dslType value, a policy map is created with a policy map name resulting in hash value 0. Because a policy map name with a hash value 0 is not handled properly by the QoS client, the router crashes.

  Conditions: This issue is observed when BRAS applies an ANCP shaper with a specific policy map name, ActualDownstreamRate, and dslType value.

  Workaround: There is no workaround.

- CSCto40479 and CSCto89992

  Symptom: During an ISSU subpackage upgrade from Release 3.2.x to Release 3.3.0, the router crashes. During an ISSU subpackage downgrade from Release 3.3.0 to Release 3.2.x, the standby RP does not come up correctly after the procedure. Instead, the standby RP reloads continuously and IPC timeout messages are generated each time the RP reloads.

  Conditions: This issue is observed when subpackage ISSU is performed on the router.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS XE Release 3.2.1S

This section documents unexpected behavior that might be seen in Cisco IOS XE Release 3.2.1S.

- CSCtl71478

  Symptom: In an HA system, the following error message is displayed on the standby RP and LC:

  ```
  OCE-DFC4-3-GENERAL: MPLS lookup unexpected
  ```

  Conditions: This issue is observed when both the RP and the standby/LC routers are brought up either with or without configuration.

  Workaround: There is no workaround.

- CSCta37670

Symptom: The router crashes when the watchdog times out.

Conditions: This issue is observed on adding a large number of routes in IXIA, which causes an increase in the size of the IP VRF table.

Workaround: There is no workaround.

- CSCtl67150

  Symptom: Multilink interfaces take more than 30 seconds to start up.

  Conditions: This issue is observed with all multilink interfaces.

  Workaround: There is no workaround. Note that the delay in starting up does not affect the working of the multilink interfaces.

- CSCto03123

  Symptoms:

  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.

  Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.

  Workaround: There is no workaround.

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

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

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

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

Resolved Caveats—Cisco IOS XE Release 3.2.1S

This section documents issues that have been resolved in Cisco IOS XE Release 3.2.1S.

- CSCta43825

  Symptom: A CMTS or SNMP walk of the ARP table causes high CPU usage.

  Conditions: This issue is observed when a CMTS or SNMP walk of the ARP table is performed.

  Workaround: To prevent an SNMP walk of the ARP table, implement an SNMP view by using the following commands:

  snmp-server view cutdown iso included

  snmp-server view cutdown at excluded

  snmp-server view cutdown ip.21 excluded

  snmp-server community public view cutdown ro

  snmp-server community private view cutdown rw

- CSCtd72318

  Symptom: The Cisco ASR 1004 Router crashes at in_be_dhcpc_for_us.

Conditions: This issue is observed in Cisco IOS Release 12.2(33)XNC2. It may be associated with the DHCP configuration.

Workaround: There is no workaround.

- CSCtd94789

  Symptom: The IPSEC rekey fails after failover when stateful IPSEC HA is in use.

  Conditions: This issue is observed when using PFS, after a failover of the hub devices.

  Workaround: If the security policy permits it, then remove the PFS.

- CSCte65688

  Symptom: When the software VPN client establishes an IPSec session, the EzVPN server prints the following message:

  ```
  Client_type=UNKNOWN message in the %CRYPTO-6-EZVPN_CONNECTION_UP: (Server) log
  ```

  Conditions: This issue is observed when EzVPN is configured between a Cisco VPN client and router and **crypto logging ezvpn** is configured.

  Workaround: There is no workaround.

- CSCtf41721

  Symptom: A DMVPNv6 hub might crash when the tunnel interface of the other hub is shut down and then restarted.

  Conditions: This issue is observed if DMVPNv6 is configured with two hubs and two spokes, and a certain set of commands are run in a specific sequence.

  Workaround: There is no workaround.

- CSCtf81621

  Symptom: Line-By-Line configuration synchronization fails, and the standby RP is reloaded.

  Conditions: This issue is observed while configuring **protocol ppp virtual-template** under the ATM PVC mode.

  Workaround: Configure **no policy config-sync lbl prc reload.**

- CSCth03022

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

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

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

- CSCti36310

  Symptom: The router might leak memory when IKE attributes are pulled by SNMP.

  Conditions: This issue is observed on a router on which SNMP is enabled.

  Workaround: There is no workaround.

- CSCti47252

Symptom: SBC can attach an adjacency even when a wrong remote address is configured for the redundant peer.

Conditions: This issue is observed when a wrong remote address is configured for the redundant peer.

Workaround: There is no workaround.

- CSCti48504

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

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

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

- CSCti54173

  Symptom: A leak of 164 bytes of memory for every packet that is fragmented at high CPU is seen after all the processor memory is leaked. This causes the router to reload.

  Conditions: This issue is observed after all the processor memory is leaked.

  Workaround: There is no workaround.

- CSCti66454

  Symptom: The router crashes when the **show crypto session detail** command is run after the **clear crypto session** command is run.

  Conditions: This issue is observed if the **clear crypto session** command is run while the router is running some form of tunnel protection.

  Workaround: After running the **clear crypto session** command, wait for at least 30 seconds before running the **show crypto session detail** command.

- CSCti94938

  Symptom: The router crashes when a nonexistent route map is applied and then modified.

  Conditions: This issue is observed when there is more than one L2TP session on the virtual template interface.

  Workaround: Configure the route map before applying the policy.

- CSCti98931

  Symptom: Some sessions may be lost after an L2TP switchover.

  Conditions: This issue is observed after an L2TP switchover.

  Workaround: There is no workaround.

- CSCtj14525

  Symptom: After a new policy is attached, the standby RP is not switched to active state in the event that the active RP crashes.

  Conditions: This issue is observed after a new policy is attached.

  Workaround: There is no workaround.

- CSCtj29831

  Symptom: The router crashes after an SSO.

  Conditions: This issue is observed when an IPv6 named and tagged ACL is applied through the service logon.

  Workaround: There is no workaround.

- CSCtj40564

  Symptom: The router does not allow an incoming IKE connection even if the keyring is matched.

  Conditions: This issue is observed after the router is reloaded and when a crypto keyring having a local address defined as an interface is used.

  Workaround: Use an IP address.

- CSCtj51139

  Symptom: ASR1000-SIP40 crashes due to a low-memory condition.

  Conditions: This issue is observed when a large number of PPPoA sessions are started on a single SIP40 with autovc and autosense configured.

  Workaround: Apply one of the following workarounds:

  - Reduce the number of sessions on a single SIP40 (14000 or fewer).
  - Enable either autovc or autosense (not both) at any point of time to reduce the number of IPC messages.

- CSCtj73848

  Symptom: The bba_ipv6_lns traffic fails after an RP switchover.

  Conditions: This issue is observed after an RP switchover.

  Workaround: There is no workaround.

- CSCtj77004

  Symptom: The size of the archive log configuration impacts CPU usage during PPPoE establishment. In addition, only some configuration lines from the virtual template are copied to the archive. The remaining lines are not copied.

  Conditions: This issue is observed when **archive log config** is configured.

  Workaround: There is no workaround.

- CSCtj82401

  Symptom: After the router is rebooted, all adjacencies get detached and all calls fail.

  Conditions: If the configured default call policy contains na-carrier-id-table, it is converted to na-dst-carrier-id-table. During reboot, na-dst-carrier-id-table is detected as an unrecognized command and that part of the configuration is rejected. This leaves SBC in a state where all adjacencies are detached until the problem is corrected.

  Workaround: Manually add na-carrier-id-table back to the configuration after reloading the router. After adding na-carrier-id-table, deactivate and then reactivate SBC.

- CSCtj82405

  Symptom: After a chassis is reloaded, the secondary IP address configured on the SBC interface is automatically removed. Because this is the media address, all subsequent calls fail because there is no functional media address.

  Conditions: This issue is observed after a chassis is reloaded.

Workaround: There is no workaround.

- CSCtj89941

  Symptom: IOS crashes when the **clear crypto session** command is used on an EzVPN client.

  Conditions: This issue is observed when the **clear crypto session** command is used on an EzVPN client.

  Workaround: There is no workaround.

- CSCtj94490

  Symptom: The RP reloads after 30 RP switchovers.

  Conditions: This issue is observed when a large number of PPPoEoA sessions are present and when traffic is flowing.

  Workaround: There is no workaround.

- CSCtj99466

  Symptom: The volume-based SA lifetime is set to 0 on almost all the sessions while bringing up a large number of SVTI tunnels on a router with RP1. This results in traffic not getting encrypted and decrypted on those tunnels.

  Conditions: This issue is observed after performing a sequence of steps that clear all crypto sessions.

  Workaround: There is no workaround.

- CSCtk00398

  Symptom: On receiving DHCPv6 SOLICIT from two clients with the same DUID, DHCPV6 binds the delegated prefix to the wrong client.

  Conditions: This issue is observed when two clients send SOLICIT messages with the same DUID.

  Workaround: There is no workaround.

- CSCtk06750

  Symptom: IP-directed broadcast packets do not get forwarded by a downstream router.

  Conditions: When link encapsulation is set to HDLC, layer frames are sent out with an incorrect address type. Therefore, the downstream router does not forward them further as directed broadcast packets.

  Workaround: Change the encapsulation to PPP on the affected serial interfaces.

- CSCtk12252

  Symptom: A Priority 1, valid SONET controller network clock source is not selected as the active clock source. Instead, the clock remains in the FREERUN state.

  Conditions: This issue is observed after the router is reloaded, and when a valid, but absent, Priority 2 network clock source is specified.

  Workaround: Shut down and then restart the near-end Priority 1 clock source SONET controller.

- CSCtk12708

  Symptom: The router crashes when the holdover clock source is deleted.

  Conditions: This issue is observed when the holdover clock source is deleted.

  Workaround: There is no workaround.

- CSCtk30508

Symptom: After a FRoMPLS PW is torn down, the connect object stays in FMAN-RP, FMAN-FP, and CPP. This causes memory leakage. It may also cause failure in creating a FRoMPLS PW.

Conditions: There are no specific conditions under which this issue is observed.

Workaround: There is no workaround.

- CSCtk30807

  Symptom: A router that acts as a DHCP relay server crashes when the DHCP service is shut down by first running the **no service dhcp** command and then restarted by running the **service dhcp** command.

  Conditions: This issue is observed when the router is also configured as the ISG.

  Workaround: There is no workaround.

- CSCtk34287

  Symptom: MFIB does not delay release of MDT adjacency when capability is configured.

  Conditions: This issue is observed when capability is configured.

  Workaround: There is no workaround.

- CSCtk35599

  Symptom: During a slow-start to slow-start H.323 call, the initial bandwidth that is requested is the same as that required for a voice call. This might cause video call degradation when interworking with VCS-E.

  Conditions: This issue is observed when interworking with VCS-E.

  Workaround: There is no workaround.

- CSCtk54431

  Symptom: When a router BRAS receives SOLICIT IA-PD from the CPE, but no Delegated-IPv6-Prefix is received from RADIUS, no reply is sent to the CPE. The expected response is that an Advertise with the NoPrefixAvail option is sent.

  Conditions: This issue is observed when the CPE requests IA-PD, but BRAS does not have a Delegated-IPv6-Prefix.

  Workaround: There is no workaround.

- CSCtk67176

  Symptom: When billing is configured, the CDR media-info CLI is not automatically enabled.

  Conditions: This issue is observed when billing is configured.

  Workaround: There is no workaround.

- CSCtk68647

  Symptom: DMVPN disallows connections after a certain number of connections are established. The **show crypto socket** command shows that sockets are leaking and do not stop even when the SA is inactive.

  Conditions: This issue is observed in releases earlier than Cisco IOS Release XE 3.2.0 and when multiple DMVPN tunnels are configured with tunnel protection shared.

  Workaround: Upgrade to Cisco IOS Release XE 3.2.0, and remove or shut down the other DMVPN tunnels.

- CSCtk75389

  Symptom: The PfR fallback interface does not remain in policy.

Conditions: This issue is observed on the ATM interface.

Workaround: There is no workaround.

- CSCtl00127

  Symptom: The output of the **show ip int** command does not indicate whether the **ip security ignore-cipso** option is configured and operational.

  Conditions: There are no specific conditions under which this issue is observed.

  Workaround: There is no workaround.

- CSCtl05979

  Symptom: In SSO mode, PPPoE sessions with PAC2 ISG service are replicated on the standby RP, with policy maps missing on the standby RP. The expected behavior is that the PAC2 service must poison the PPPoE sessions.

  Conditions: This symptom is observed in SSO mode, when PPPoE sessions with the PAC2 ISG service are established.

  Workaround: Use the dummy ISG service applied from RaBaPol to force poisoning.

- CSCtl08014

  Symptom: The router crashes with memory corruption symptoms.

  Conditions: This issue is observed when performing switchover or OIR when MLP sessions are getting initiated.

  Workaround: There is no workaround.

- CSCtl20993

  Symptom: The router crashes during IPsec rekey.

  Conditions: There are no specific conditions under which this issue is observed.

  Workaround: There is no workaround.

- CSCtl49769

  Symptom: SBC does not report the media address in a Lawful Intercept IRI message. In a Lawful Intercept environment, the expected behavior is that the media IP address and port details of the parties in the call must be reported to the MF so that the Call Content-tapped traffic can identify the direction of the media flow.

  Conditions: This issue is observed during normal call flow.

  Workaround: There is no workaround.

- CSCtl50930

  Symptom: For some SIP messages (for example, OPTION), SBC asserts failure when the call is sent through VRF.

  Conditions: This issue is observed on the Cisco ASR 1001, 1002, and 1004 Routers in nonredundant mode.

  Workaround: Configure redundant mode SSO.

- CSCtl83053

  Symptom: The Shaper rate cannot be changed by using ANCP Port Up messages.

  Conditions: This issue is observed on a router with QOS and ANCP enabled.

  Workaround: There is no workaround.

- CSCtl42358

  Symptom: The router crashes after the `no atm sonet overhead j1` message is issued.

  Conditions: There are no specific conditions under which this issue is observed.

  Workaround: There is no workaround.

- CSCtl74301

  Symptom: INBOX SSO does not work on the Cisco ASR 1006 Router. When this occurs, SSO drops signaling and RTP.

  Conditions: This issue is observed during INBOX SSO. This occurs when SIP binds with the loopback address for control.

  Workaround: There is no workaround. Unless required by your network architecture, do not use a loopback address for control bind.

- CSCtd16959

  Symptom: Traceback is seen on SSO switchover.

  Conditions: This issue is observed when the following steps are performed:

  - The CBTS master tunnel is configured with three member tunnels.
  - The member tunnels are deleted and then the master command is removed from the master tunnel so that it becomes a regular TE tunnel.
  - The auto-tunnel primary and backup setup are configured.
  - SSO switchover is performed.

  Multiple tracebacks are seen on the newly active RP, which are related to MPLS TE.

  Workaround: Do not delete the CBTS tunnels.

- CSCte51529

  Symptom: CUBE does not forward 491 Request Pending responses.

  Conditions: This issue may be observed during a consultative call transfer flow.

  Workaround: There is no workaround.

- CSCtf23298

  Symptom: There is high CPU usage when a TACACS server is configured with a single connection.

  Conditions: This issue is observed when a TACACS server is configured with a single connection.

  Workaround: Remove the single connection option.

- CSCtf72328

  Symptom: The BFD IPv4 Static feature does not fully support the Administratively Down status.

  Conditions: This issue is observed because the BFD APIs do not notify its clients about the Administratively Down status. If the clients do not receive notification about the BFD peer Administratively Down status, then they consider the BFD peer to be up and running.

  Workaround: Shut down and then restart the interface on which the BFD session is configured.

- CSCtg28806

  Symptom: The router crashes during PKI manual enroll.

  Conditions: This issue is observed on a router running Cisco IOS Release 15.0(1)M1.

  Workaround: There is no workaround.

- CSCtg64175

  Symptom: The IS-IS route is missing the P2P link. It is incorrectly marked as `parallel p2p adjacency suppressed`.

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

  Workaround: Shut down and then restart the local P2P interface.

- CSCth13415

  Symptom: One-way audio in call transfer due to 491 response during resume re-INV.

  Conditions: This issue is observed when there is an UPDATE message passing through the CUBE and then a re-INV crossover occurs. The re-INV crossover results in a 491, but the 491 is not correctly forwarded by the IPIP GW. This may result in one-way audio if the crossed-over re-INV was in the process of changing the state of the media from Hold to Resume.

  Workaround: There is no workaround.

- CSCth37580

  Symptom: The dampening route is present even after removing BDP dampening.

  Conditions: This issue is observed under the following conditions:

  - DUT connects to RTRA with eBGP VPNv4.
  - eBGP VPNv4 peer session is established and DUT.
  - DUT has VRF (same RD) as the route advertised by RTRA. In this scenario, when DUT learns the route it performs the same RD import. In addition, the topology of the net is changed from VPNv4 to VRF.

  Workaround: There is no workaround.

- CSCth61759

  Symptom: Video call fails with CVTA.

  Conditions: This issue is observed when there is an end-to-end SIP flow around the call with CVTA.

  Workaround: There is no workaround.

- CSCth93218

  Symptom: The `%OER_BR-4-WARNING: No sequence available` error message is displayed on PfR BR.

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

  Workaround: There is no workaround.

- CSCti08811

  Symptom: The router may reload when running commands through an Embedded Event Manager (EEM) policy.

  Conditions: This issue is observed only when EEM policies are used.

  Workaround: There is no workaround.

- CSCti22091

Symptom: Traceback occurs after the **show oer master** command is used a few times. The traceback is always followed by the `learning writing data` message. The traceback causes the OER system to be automatically disabled. Manually re-enabling PfR does not work, and a reboot is required.

Conditions: This issue is observed when the following procedure is performed:

3. In the list submode of PfR, a traffic-class application is configured with a prefix list as the filter.
4. In the traffic-class submode of PfR, keys are configured and then an ACL is configured as a filter.

Workaround: There is no workaround.

- CSCti25319

  Symptom: A directly connected subnet that is covered by a network statement is not redistributed into another routing protocol, even if a redistribute OSPF is configured.

  Conditions: This issue is observed only on configurations in which a network mask covers multiple supernets.

  Workaround: Apply one of the following workarounds:

  – Enable OSPF using the **ip ospf** *AS* **area** interface command.
  – Configure multiple network statements with the mask/wildcard equal to the supernet as shown in the following example:

    router ospf 1 network 192.168.0.0 0.0.0.255 area 0 network 192.168.1.0 0.0.0.255 area 0

- CSCti34396

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

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

  Workaround: Apply one of the following workarounds:

  – Configure a route-map to rewrite routes so that the tunnel endpoint is an address reachable from both inside the VRF and outside it.
  – Instead of configuring static routes with a next-hop, specify an interface name.

- CSCti51145

  Symptom: After a reload of one router, some or all of the BGP address families do not become active. The output of the **show ip bgp all summary** command shows the address family in NoNeg or Idle state, and it remains in that state.

  Conditions: This issue is observed when all of the following conditions are met:

  – The non-reloading device has a **neighbor x.x.x.x transport connection-mode passive** configuration. Alternatively, there is an IP ACL or packet filter that permits connections initiated by the reloading device, but not by the non-reloading device.
  – The BGP hold time that is configured is less than the time required for neighbor x.x.x.x to reload.
  – When neighbor x.x.x.x reloads, no keepalives or updates are sent on the stale session during the interval between the time the interface comes up and neighbor x.x.x.x exchanges BGP open messages.
  – Both peers are multisession capable.
  – The **transport multi-session** setting is not configured or enabled by default on either device.

  - The **graceful restart** setting is not configured.

  Workaround: Apply one of the following workarounds:

  - Remove the **neighbor x.x.x.x transport connection-mode passive** configuration or edit the corresponding filter or IP ACL to permit the active TCP to open in both directions.
  - Configure the **neighbor x.x.x.x transport multi-session** setting on either the device or its neighbor.
  - Configure a very short keepalive interval (such as 1 second) on the nonreloading device by using the **neighbor x.x.x.x timers 1 holdtime** command.
  - Configure graceful restart by using the **neighbor x.x.x.x ha-mode graceful-restart** command.
  - If this issue occurs, use the **clear ip bgp *** command to cause all sessions that are in the NoNeg state to restart. Alternatively, you can use the **clear ip bgp x.x.x.x addressFamily** command to bring up individual sessions without resetting everything.

- CSCti61949

  Symptom: The router reloads and the `SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header` and `chunk name is BGP (3) update` messages are displayed.

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

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

- CSCti67102

  Symptom: A tunnel is automatically disabled due to the creation of a recursive routing loop in RIB.

  Conditions: This issue is observed when a dynamic tunnel that is passive by default is created. EIGRP receives a callback due to the address change (dynamic tunnel comes up). EIGRP tries to run on this interface and install an EIGRP route in the RIB, which replaces the tunnel next-hop.

  Workaround: There is no workaround.

- CSCti68721

  Symptom: The output of the **show performance monitor history interval <all | given #>** command shows an extra column.

  Conditions: This issue is observed when traffic runs on a performance monitor policy at the time when a user runs the **show** command.

  Workaround: Repeat the command when this issue is observed.

- CSCti81136

  Symptom: Running the **no ip route-cache** command on an interface results in both **no ip route-cache** and **no ip route-cache cef** appearing in the configuration.

  Conditions: This issue is observed when the **no ip route-cache** command is run on an interface.

  Workaround: There is no workaround.

- CSCti84762

  Symptom: Update generation does not proceed, and some peers remain in the refresh started state (SE).

  Conditions: This issue is observed when there is peer flap, route churn, or interface flap.

  Workaround: Hard reset the peers that are in the SE state.

- CSCti85446

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

Conditions: This issue is observed after the following sequence of actions and events:

1. A next-hop static route is configured with a permanent keyword.
2. The next-hop IP address becomes unreachable.
3. Change the configuration in such a way that the next-hop is reachable.
4. Configure a new static route through the next-hop IP address used in step 1.

Workaround: Delete all the static routes through the affected next-hop, and then add them again.

- CSCti91215

  Symptom: The router stops responding.

  Conditions: This issue is observed while removing the address family a second time.

  Workaround: There is no workaround.

- CSCti92450

  Symptom: OSPFv3 graceful restart does not terminate gracefully because it remains in pending state on a loopback interface.

  Conditions: This issue is observed when there is at least one loopback interface with OSPFv3 configured.

  Workaround: There is no workaround.

- CSCtj05670

  Symptom: During SSO with scaled mLDP configuration, the path set for some VRFs are not configured.

  Conditions: This issue is observed while configuring mLDP on 100 VRFs with 100 receivers.

  Workaround: There is no workaround.

- CSCtj08533

  Symptom: QoS classification fails on the egress PE if the route is learned through BGP.

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

  Workaround: Use only one path between the PE and CPE.

- CSCtj11322

  Symptom: The AAA server is not able to decode RADIUS attributes.

  Conditions: There are no specific conditions under which this issue is observed.

  Workaround: There is no workaround.

- CSCtj17316

  Symptom: EIGRP flaps in a large-scale network with a large amount of traffic.

  Conditions: This issue is observed in a large-scale network with a large amount of traffic.

  Workaround: Apply one of the following workarounds:

  - Find the instability in the network, and fix the interface.
  - Summarize the routes.
  - Change more routers to stub.
  - Upgrade to Release 7 of EIGRP.

- CSCtj17545

  Symptom: After a switchover, the restarting speaker sends TCP-FIN to the receiving speaker when the receiving speaker tries to establish a connection. This may cause packets to be dropped after the switchover.

  Conditions: This issue is observed when a large number of BGP peers are established on different interfaces.

  Workaround: Configure the receiving speaker to accept passive connections.

- CSCtj24453

  Symptom: Traceback is observed when the **clear ip bgp *** command is run.

  Conditions: This issue is observed when there are relatively few routes and route-map-cache entries.

  Workaround: Use the **no bgp route-map-cache** command.

- CSCtj28747

  Symptom: Route control of prefix and application are out of order. This makes application control ineffective. The `Exit Mismatch` message is logged, and the application becomes uncontrolled for a short interval before it comes back under control.

  Conditions: This issue is observed only if PIRO control is used where prefixes are also controlled using dynamic PBR.

  Workaround: There is no workaround.

- CSCtj32574

  Symptom: Removal of the **redistribute** configuration in EIGRP is not synchronized to the standby RP.

  Conditions: This issue is observed when any redistribute-related command is run.

  Workaround: There is no workaround.

- CSCtj32769

  Symptom: Data path fails with L2VPN on an ACR interface.

  Conditions: This issue is observed when a VPN is configured on an ACR interface in asynchronous mode with cell-packing configurations. This issue is not observed in normal synchronous mode or L2VCs.

  Workaround: Configure the same MNCP value for local and remote PE devices.

- CSCtj36521

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

  Conditions: This issue is observed only if IPv6 CEF is enabled at the same time.

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

- CSCtj38579

  Symptom: FlexWan crashes continuously with Tunnel QoS.

  Conditions: This issue is observed with pim-register ratelimit.

  Workaround: There is no workaround.

- CSCtj45084

Symptom: A crash occurs when the **clear ip ospf process** command is run in a multicast configuration.

Conditions: This issue is observed when the **clear ip ospf process** command is run in a multicast configuration.

Workaround: There is no workaround.

- CSCtj47736

  Symptom: The router crashes when the **show eigrp service ipv4 neighbor** command is run.

  Conditions: This issue is observed when the neighbor is learned, you add a max-service limit on an address family, and you then shut down and restart the interface.

  Workaround: There is no workaround.

- CSCtj48629

  Symptom: Although the **ppp multilink load-threshold 3 either** setting is configured, member links are not added by the inbound heavy traffic on the PRI of the HWIC-1CE1T1-PRI.

  Conditions: There are no specific conditions under which this issue is observed.

  Workaround: There is no workaround.

- CSCtj52564

  Symptom: The router crashes when removing the pppoe-client configuration from the VC.

  Conditions: This issue is observed when you try to remove the pppoe-client configuration by running the **no pppoe-client** command on the VC.

  Workaround: There is no workaround.

- CSCtj58943

  Symptom: The standby RP reloads due to line-by-line sync failure when the **encapsulation dot1q 1381** command is run.

  Conditions: This issue is observed when a configuration command is run in the subinterface mode.

  Workaround: There is no workaround.

- CSCtj64728

  Symptom: After the VNET tag value is reconfigured, a member switch console cannot be accessed after stack bootup.

  Conditions: This issue is observed after the VNET tag value is reconfigured.

  Workaround: There is no workaround.

- CSCtj64940

  Symptom: When a police rate is set for values more than 4 Gbps (for example, on 10 Gbps Ethernet), the actual rate is incorrectly set to some random value.

  Conditions: This issue is observed only when police rate configurations are more than 4 Gbps.

  Workaround: There is no workaround.

- CSCtj65553

  Symptom: A static route entry created in the default table is automatically deleted.

  Conditions: This issue is observed after a Route Processor to Line Card to Route Processor transition on the Cisco Catalyst 3000 series switching module.

  Workaround: Manually configure the missing static route.

- CSCtj67794

  Symptom: IPv6 multicast RPF lookup fails when the primary static default route is unreachable and replaced by the standby static route.

  Conditions: This issue is observed when two or more IPv6 static routes are configured as the default route with metric. After the primary default route is lost and replaced by the standby static route, multicast RPF fails and multicast traffic is affected.

  Workaround: Configure a static default route with an outgoing interface.

- CSCtj72730

  Symptom: When an EIGRP address-family configuration is removed, a redistribution command that refers to the address-family is not removed. The expected behavior is that all redistribution commands should be removed.

  Conditions: This issue is observed when an EIGRP **address-family** configuration command is removed.

  Workaround: Manually remove the redistribution commands that are not removed after the **address-family** command is removed.

- CSCtj74570

  Symptom: The router crashes when trying to check the PVC command syntax in the syntax check mode.

  Conditions: This issue is observed when you try to run the **pvc** command in the syntax check mode without having a PVC created during configuration that is carried out before the syntax check.

  Workaround: There is no workaround.

- CSCtj79750

  Symptom: Multicast responses are not received.

  Conditions: After a Multicast Listener Discovery (MLD) join, multicast responses are not received.

  Workaround: There is no workaround.

- CSCtj82292

  Symptom: EIGRP summary address with AD 255 are sent to the peer.

  Conditions: This issue occurs when a summary address is advertised as shown in the following example:

  ```
  ip summary-address eigrp AS# x.x.x.x y.y.y.y 255
  ```

  Workaround: There is no workaround.

- CSCtj84389

  Symptom: A member switch console cannot be accessed after stack bootup.

  Conditions: This issue is observed when IEEE 802.1x is configured.

  Workaround: There is no workaround.

- CSCtj87180

  Symptom: When an LAC router receives an invalid redirect from a peer running VPDN, it may crash with the following CDN error message:

  ```
  SSS Manager Disconnected Session
  ```

  Conditions: This issue is observed when the LAC router receives an incorrect error from the multi-hop peer.

Workaround: There is no workaround.

- CSCtj92379

  Symptom: The router might crash when CEF forwarding is enabled.

  Conditions: CEF optimise neighbour resolution must be enabled for the address family (IPv4 or IPv6). A packet destined for an unknown neighbor on an Ethernet interface matches the connected prefix for that Ethernet, and triggers a glean operation.

  Workaround: Depending on the address family whose CEF is forwarding, apply one of the following configurations:

  no ip cef optimize neighbor resolution

  no ipv6 cef optimize neighbor resolution

- CSCtj96915

  Symptom: The LNS router stops responding at interrupt level and enters an infinite loop.

  Conditions: There are no specific conditions under which this issue is observed.

  Workaround: There is no workaround.

- CSCtj97823

  Symptom: Topology names that are 32 bytes long are not handled correctly on bootup.

  Conditions: This issue is observed when 32-byte topology names are used.

  Workaround: Use topology names that are shorter than 32 bytes.

- CSCtk00487

  Symptom: When an L3 port that is configured with the **ip igmp join-group** command is converted into an L2 port, multicast traffic is punted to the CPU.

  Conditions: This issue is observed when the L3 port has **ip igmp join-group** configured for a group for which there are multicast sources. Later, the L3 port is converted into an L2 port participating in a VLAN that is either a source or receiver of that group.

  Workaround: Apply one of the following workarounds:

  - Remove the **ip igmp join-group** configuration before converting the port to an L2 port.
  - Convert the L2 port back to an L3 port, remove the **ip igmp join-group** configuration, and then convert the port back to an L2 port.

- CSCtk00537

  Symptom: The IPv6 PIM register fails after an SSO. This results in S and G multicast routes disappearing from the last hop router (LHR). Because of this condition, traffic flow stops abruptly.

  Conditions: This issue is observed after an SSO.

  Workaround: There is no workaround. The LHR must be reloaded to fully restore the original condition.

- CSCtk00976

  Symptom: When the file descriptor reaches the maximum threshold limit, you cannot save the configuration or perform any file system-related operation because file descriptors are exhausted. The `File table overflow` error is displayed.

  Conditions: This issue is observed on running the **dir/recursive <>** command periodically using the ANA tool.

Workaround: Do not run the **dir/recursive <>** command if leaks are detected. In addition, if the command is running through ANA server polling, disable it.

- CSCtk02647

  Symptom: On an LNS that is configured for L2TP aggregation, per-user ACLs downloaded through RADIUS might cause PPP negotiation failures (that is, IPCP is blocked).

  Conditions: This issue is observed when the LNS multilink is configured and negotiated for PPP/L2TP sessions, and per-user ACLs are downloaded for PPP users through RADIUS.

  Workaround: There is no workaround.

- CSCtk12608

  Symptom: Route watch fails to notify the client when a RIB resolution loop changes. This causes unresolved routes to stay in the routing table.

  Conditions: This issue is observed on certain router configurations.

  Workaround: Use static routes that are associated with a specific interface.

- CSCtk47891

  Symptom: Traffic might be lost when the LC is reset.

  Conditions: This issue is observed when Fast Reroute (FRR) is configured and it is in active state when the LC is reset.

  Workaround: There is no workaround.

- CSCtk53463

  Symptom: To configure the **shape average** *cir_value bc_value* command, *bc_value* is limited by 4 milliseconds x *cir_value*. The 4 milliseconds represent the minimum interval time for bursts. However, the ES LC can support an interval value that is faster (that is, has a smaller interval) than 4 milliseconds. This is not the expected behavior for ES LC.

  Conditions: This issue is observed when the interval time for the **shape** setting is restricted from dropping below 4 milliseconds.

  Workaround: There is no workaround.

- CSCtl08601

  Symptom: Unconfiguring the DHCP pool causes the console to stop responding.

  Conditions: This issue is observed when the **no service dhcp** command is run before the pool is unconfigured.

  Workaround: There is no workaround.

- CSCtd54703

  Symptom: When the tunnel interface of a spoke is shut down and then restarted, the router crashes.

  Conditions: This issue is observed when the IPv6 NHRP cache fails and the tunnel interface of a spoke is shut down and restarted.

  Workaround: There is no workaround.

- CSCtk53606

  Symptom: When the router is inserted either as a probe source or a responder, a high maximum RTT value is seen for the UDP Jitter probe.

  Conditions: This issue is observed when running UDP Jitter probes.

  Workaround: There is no workaround.

- CSCtj85638

  Symptom: Following a change to an ACL or prefix-list referenced by an OSPF **distribute-list...in** command, OSPF routes may be lost from the RIB.

  Conditions: This issue is observed in configurations that use a distribute list to filter routes that OSPF installs in the RIB.

  Workaround: Allow at least 10 seconds between successive changes to the ACL or prefix-list.

- CSCth69364

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

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

- CSCti80847

  Symptom: In a DVTI EzVPN setup, if the client sets the peer address to the secondary IP address of a loopback interface on the server, then the established IPSEC tunnel will not have the correct MTU value.

  Conditions: This issue is observed when the secondary IP address of the loopback is used as the IPSec tunnel end address.

  Workaround: Do not use the secondary IP address of the loopback as the IPSec tunnel end address.

- CSCtb89745

  Symptom: RRI functionality does not work as expected.

  Conditions: This issue is observed when the router is running in the HA Pair mode.

  Workaround: Add the crypto ACL again to populate the IP routes.

- CSCti79478

  Symptom: The serial interface is not attached to the OSPF process after reload even though there is a network statement to cover the interface.

  Conditions: This issue is observed when the serial interface is configured as an unnumbered interface.

  Workaround: Remove the **ip unnumbered** configuration, and then reapply it for the interface.

- CSCtf71673

  Symptom: A PRE crash occurs because of memory corruption caused by a block overrun.

  Conditions: This issue is observed when the router is configured for PTA and L2TP access and the router receives a PADX packet whose actual length is more than the length given in pppoe_header.

  Workaround: There is no workaround.

- CSCta11223

  Symptom: The router may crash when the **show dmvpn** or **show dmvpn detail** command is run.

  Conditions: This issue is observed when DMVPN is configured and the **show dmvpn** or **show dmvpn detail** command is run multiple times.

  Workaround: There is no workaround.

- CSCtk12018

  Symptom: The ESP crashes when a tunnel interface is recursively shut down and restarted.

Conditions: This issue is observed when the tunnel interface is recursively shut down and restarted.

Workaround: There is no workaround.

- CSCtl59149

  Symptom: When the Idle Peer Detect (IPD) feature is configured on an IPSec session, failover of the ESP may not be stateful. Some IPSec sessions may be torn down and re-created during the failover.

  Conditions: This issue is observed when the IPD feature is configured on the IPSec session.

  Workaround: There is no workaround. Note that the IPSec sessions that are torn down start up automatically after the failover of the ESP.

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

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

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

Open Caveats—Cisco IOS XE Release 3.2.0S

This section documents unexpected behavior that might be seen in Cisco IOS XE Release 3.2.0S.

- CSCth03302

  After RP switchover, IPv6 traffic on RBE subinterface recovers after few seconds.

  This condition has been observed when IPv6 is configured on RBE VCs and RP switchover has occurred.

  Workaround: There is no workaround.

- CSCth08313

  IPC Periodic Timer Driver MSG error has been observed on the Cisco ASR 1000 Router.

  The following error message has been seen during online operations:

  ```
  : %SYS-SP-2-GETBUF: Bad getbuffer, bytes= 24616 -Process= "IPC Periodic Timer", ipl=
  0, pid= 24-Traceback= 81745F8 81D19E8 8BEAD94 8BEB5C4 853BAD4 8527704 854CE24 82AE1B0
  82AE2E8 855E454 835AFD0 83552E8
  Or
  IPC: Sending Big IPC msg to Driver MSG: ptr: 0x152CDAC8, flags: 0x14328, retries: 1,
  seq: 0x2016C68, refcount: 2, rpc_result = 0x0, data_buffer = 0x14FB3084, header =
  0x78730658, data = 0x78730678 || HDR: src: 0x216001E, dst: 0x2010000, index: 0, seq:
  27752, sz: 1808, type: 14209, flags: 0x1608, ext_flags: 0x0, hi: 0x1B622B, lo:
  0x36C456 || DATA: 00 00 00 06 0E 19 00 08 00 00 00 00 00 00 03 12 00 00 00 00 89 00 00
  00 00 00 00 00 00 06 E8 00 00 00 01 11 9E 04 34 04 60 08 00 00 01 00 20 6E 00 67 05
  EF E8 00 06 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 16
  This has been seen either after boot of the router or after failover.
  ```

  Workaround: There is no workaround.

- CSCth11310

IP-subscriber sessions stop forwarding traffic after RADIUS proxy resets them. The session does not appear to get any traffic, and drops may be observed when the following command is used:

show platform hardware qfp active statistics drop

This behavior may occur on ASR 1000 Router Series, with routed IP-subscriber sessions that are reset and converted to RADIUS proxy sessions.

Workaround: There is no workaround.

- CSCth14949

  After enabling ip tcp header-compression when POS is configured on the interface a traceback has been seen.

  This condition may occur only when POS is configured on the interface and ip tcp header-compression enabled.

  Workaround: Do not enable ip tcp header-compression when POS is configured on the interface.

- CSCth22250

  On 2RU-F and ESP-5 when bringing up translations at higher rate, all sessions cannot be established.

  This conditions has been observed on 2RU-F and ESP-5 when bringing up translations at higher setup rate.

  Workaround: Is to lower the setup rate.

- CSCti03323

  It takes the ESP about 1 minute longer to become fully active after an ISSU load version event.

  This only occurs during ISSU process and increases with more linecards.

  Workaround: There is no workaround

- CSCti14975

  Tracebacks may be seen on Cisco ASR 1006 with RP2 while removing any security ACL.

  A failure may be observed when issuing the "**show access-list**" command while running Cisco IOS XE 3.2.1S release.

  This condition may occur when traceback is seen when unconfiguring a security ACL on RP2.

  A failure may be observed with ACLs on per-user sessions at 3K and 32K.

  Workaround: The router works normal, just traceback is seen.

  For now, do not issue "**show access-list**" command.

- CSCti17802

  The following log message may be incorrectly displayed to prompt the user to issue 'issu runversion' in cases where the ISSU upgrade has been aborted due to the following error:

  ```
  ISSU_PROCESS-SP-7-DEBUG: Peer state is [ STANDBY HOT ]; Please issue the
  runversion command
  ```

  Wrong message is shown when ISSU gets aborted after 'issu loadversion'.

  Workaround: No workaround. This behavior has no functional impact.

- CSCti22164

  ATM PVC with AC are up for ima-acr interface even if the controller is down.

This condition may occur when ATM PVC and attachment circuit are up for the ima-acr interface even though the controller is down for the IMA-ACR interface. The controllers are down as there is mismatch for the channel/port on the peer.

Workaround: No Workaround

- CSCti27214

  BFD with Routing flap, packet loss maybe seen on Standby RP.

  This may occur when the standby RP is booting up.

  Workaround: Disable both QoS (containing NBAR) and NBAR protocol discovery from all interfaces.

- CSCti31070

  Traceback may occur while performing downgrade to a lower version of image.

  This instance has been observed after issuing **runversion** while performing downgrade to a lower version of image.

  Workaround: There is no workaround.

- CSCti34437

  QFP Tracebacks are seen after switchover for an active SRTP call.

  This condition has been observed during Switchover with SIP-SIP and SRTP-SRTP basic audio calls.

  Workaround: There is no workaround.

- CSCti50692

  ESP may reload when activating 4 template services.

  This condition has been observed when the following steps have occurred:

  1. Activate template service A in one CoA.
  2. Activate services B, C and D in another CoA.
  3. Loss of connectivity on the ESP may occur when activating template services.

  Workaround: There is no workaround.

- CSCti53718

  Newly added StandbyESP is unable to activate during init state, after performing “**issu runversion”** command.

  This conditions has been seen when bringing up 2 pppoeoa sessions and performing "issu runversion" command.

  Workaround: There is no workaround.

- CSCti59758

  Distributed SBC reserves transcoding resources for a non-transcoded call.

  This symptom is observed on distributed SBC on the ASR 1000 platform with DSP-SPA when SDP includes rtpmap and ptime information.

  Workaround: There is no workaround.

- CSCti59760

Under Cisco ASR 1000 Router B2B inter-chassis application redundant mode for CUBE-SP, it is seen that not all SBC related configuration changes made on the Active device gets auto-sync'd to the running-config on the Standby Device. Some examples of this are add/delete/edit of adjacency config and add/delete/edit of CAC and call policies. Thus the running-config between the Active and Standby devices may be out-of sync. If running-config is saved to the startup config this can result in discrepancies between the startup-config on the Standby device and startup config on the Active device.

Although this discrepancy in the replication of SBC config does affect the running-config on the Standby device, it will NOT affect the accuracy of the Standby device upon application failover. Running-config is not used by the Standby device under scenario of application failover, only upon bootup. Application failover will execute successfully.

This has been seen when CLI edits for SBC performed on the Active device under inter-chassis HA mode of CUBE-SP application.

Workaround: This issue does not affect the functionality of SBC upon application failover, only the accuracy of the SBC running-config on the Standby device. Workaround is to manually insert startup config on the Standby device w/ accurate reflection of Active SBC config rather than writing running-config to startup-config, which could inadvertently result in inaccurate SBC config upon reboot

- CSCti63058

  The CPS rate for Generic LAC and LNS sessions is about 5% less than what we had in prior releases.

  This is specific to Generic LAC and LNS while bringing up the sessions in a specific setup.

  Workaround: There is no known workaround.

- CSCti65517

  DSP SPA may not activate after proper bootup if HOT inserted into ASR 1000 SIP-X line-card following removal of a previously inserted with active SPA from the same subslot.

  Error looks similar to the example, below:

  Aug 30 15:24:37.020: %DSP-3-TIMER: SIP0/3: Bootp timer expired for DSP 0

  .....

  This condition is seen under hot SPA OIR scenario, if an active SPA is removed from an ASR1k SIP-X line-card and replaced by DSP SPA, the DSP SPA may not activate after proper bootup.

  Workaround: Reload the SIP-X line-card via cli: "**hw-module slot <slot-num>**".

- CSCti70703

  The ASR 1000 Router may reload when multiple H.323 calls made through ZBFW.

  This has been seen when ZBFW configured to inspect H.323 traffic and multiple H.323 calls are going through the system.

  The root cause analysis showed that this issue can happen with NAT configuration. also.

  Workaround: There is no workaround.

- CSCti70743

  Under B2B inter-chassis HA scenario for CUBE-SP while using SBC application, after execution of RCP to copy files to and from the Cisco ASR 1000 chassis may result in trigger of application failover.

  This condition is seen under inter-chassis HA with B2B scenario for CUBE-SP while using SBC application along with execution of 'copy rcp:... local-loc'.

Workaround: There is no workaround.

- CSCti71739

  Rekey is not getting to the Cisco ASR 1000 Router from GETVPN KS.

  This may happen when the ASR 1000 Router's and GM's are connected back to back.

  Workaround: There is no workaround.

- CSCti75302

  RP failure (during Punt Keepalive process) is observed after a longevity Test with BGP, OSPF, and Multicast configurations.

  This conditions has been observed after a longevity test. This problem has been identified as a possible ESP memory leak which would may cause Active RP to crash (RP1 and RP2), and due to this leak the RPs may continue to have failures every three hours causing a network outage.

  In addition, there are multiple scale features enabled at the time of failure which includes 200 BGPv4 sessions, 800 OSPF sessions, 500 IGMPv2 groups with PIM and 50 RSVP sessions.

  Workaround: There is no workaround.

- CSCti80847

  In a dVTI + EZVPN setup, if client sets the peer address to the secondary ip address of a loopback interface on the server, then the established IPSEC tunnel will not have the correct MTU value.

  This is not a very common configuration, one primary address is sufficient to support multiple clients. There is no need to use the secondary address for this case.

  The existing ASR implementation uses the ip MTU of the tunnel source interface as the base of the IPSEC MTU. If client set peer to a secondary ip address on server, then MTU is mistakenly set based on a large default value, instead of base on the correct tunnel source interface.

  Workaround: Do not use secondary ip of loopback as ipsec tunnel end address.

- CSCti87639

  Standby RP reloads due to config out of sync or keepalive failure in RPR mode.

  This condition may occur when Standby RP reloads due to keepalive failure in RPR mode. This issue is observed while running nbar scripts or sometimes even with no activity on box. It cannot be reproduced manually.

  Workaround: Operate in SSO mode.

- CSCtj02412

  On the Cisco ASR 1000 Router configured with the following:

  1. Three policy maps: P1, P2, P3.
  2. Policy map P1 is applied under multilinkPPP interface. P2 and P3 not applied under any interface.
  3. Policy map P2 has one class which matches protocol.
  4. While configuring P2 as a child policy of P3 gives an error:

  The following error may appear on the console: NBAR is not supported on Multilink1.

  This problem occurs only when P1 has already applied under mulilinkPPP interface and P2 has one class which matches protocol (NBAR).

  Workaround: Remove P1 from multilinkPPP interface, then configure P2 as child policy of P3. Now apply P1 under multilinkPPP.

- CSCti96774

  Inbound ACL will be deleted from session.

  This condition is observed when performing CoA after applying an outbound ACL to the same session (with IPv6 and av-pair configured on the router).

  Workaround: Re-apply inbound ACL or in and out at the same time.

- CSCtj05507

  Stale objects have been seen when SSO is configured on an Cisco ASR 1000 Router.

  Workaround: There is no workaround.

- CSCtj05670

  When doing SSO with scaled mLDP configuration, path set for some of the VRFs are not configured.

  This issue only occurs when configuring mLDP on 100 VRFs with 100 receivers.

  Workaround: There is no workaround.

- CSCtj12161

  Validation of SIP message header may cause loss of activity on the Cisco ASR 1000 Router Series, intermittently.

  This condition may be seen when simulate SIP calls between SIP client and SIP server (Cisco ASR 1000 Router Series).

  For example:

  ```
  Validation of SIP invite message header sent fails
  Validation Failed <<< NT/OR is NOT FOUND on Side B
  ```

  Workaround: There is no workaround.

- CSCtj14778

  H323 call setup may lose connection for 1000+ consecutive calls.

  This has been observed when H323 call setup is configured for 1000+ consecutive calls.

  Workaround: Clear nat transalations in UUT and the next 1000 calls would pass. In addition, by reducing the nat TCP timeout value (for example: 5 min) will resolve this issue.

- CSCtj15181

  SMAND reloads when issuing "**sh policy-map type inspect zone-pair**"command.

  Workaround: Use HSL for retrieving zone-pair information.

- CSCtj18999

  ESP reloads with 13.5k concurrent sip calls without RTP and with CPS=2k in NAT only configuration.

  Workaround: Use less CPS.

- CSCtj23259

  The ASR 1000 Router acts as a PE and has scaled configs for L2TPv3 feature combination with EoMPLS and ATMoMPLS with 2000 Pseudowires. CC failure is observed when doing CC OIR.

  This condition may occur when doing CC OIR and the CC failure is observed. This maybe seen only when the SIP is using SPA-1XCHOC12/DS0 or SPA-2XOC3-POS spa's on the router. This has not been observed with other types of SPAs.

Workaround: There is no workaround.

- CSCtj30897

  Alterations made to dspfarm resources (without first de-activating SBC application) for ***maximum sessions x***an cause SBC to stop processing new transcoded calls and also SBC does not apply the newly configured changes immediately.

  This condition has been observed when alterations to ***dspfarm profile x transcode***without first de-activating SBC application can cause SBC to stop processing new transcoded calls.

  Workaround: De-activate SBC application (via ***no activate*** cli) prior to making any changes to dspfarm resources. If this is done, upon re-activation of SBC, dspfarm changes will be applied immediately and SBC will process new incoming transcoded calls without issue.

- CSCtj30936

  H.323 tol SIP interworking performance degradation.

  This instance is observed with CPS=29/CHT=180 on Cisco ASR 1006 RP1 with ESP-10, there is TCP connection setup failure between H.323 endpoint and the ASR 1000 Router, thus causes H323 to SIP calls failure.

  Workaround: There is no workaround.

- CSCtj31470

  Multicast ping failure may occur when complex CEF options are on.

  The detailed command is "**ip cef accounting per-prefix non-recursive prefix-length load-balance-hash**".

  This condition has been observed when the ASR 1000 Router is using 12.2(33)XNE image.

  Workaround: There is no workaround.

- CSCtj35914

  In a setup with primary CEM PW and a backup configured, the traffic flows in the backup path when the primary is still up.

  This condition has been observed when reloading the module on the peer PE, when the primary path and controller is down. Allow the back up path to come up when primary path is still down. Bring up the primary path now, the traffic will not be switched to the primary path, it still flows in the back up path, though the primary path is up.

  The traffic does not switchover to primary, even if the back up path goes down.

  Workaround: Reset the module on the peer PE again when the primary controller / path is up.

- CSCtj42023

  Tracebacks with cef-mpls debug enable and disable failure may occur with sip calls.

  This condition has been observed when enabling and disabling after initiating the following:

  "debug platform hardware qfp active feature cef-mpls datapath ip all"

  Workaround: Do not send bulk traffic after enabling debug.

- CSCtj43730

  When QFP failure has occurred the call is lost and the ESP may reload.

  This condition has been observed in a environment with SRTP - SRTP calls.

  Workaround: There is no workaround.

- CSCtj44326

When issuing "**show platform hard slot p0 fan status**" command the following message for the fan speed is incorrectly shown on the console:

```
Fan group 1 speed: 166%
Fan group 2 speed: 6%
Fan 0: Normal
```

This instance maybe seen when issuing "**show platform hard slot p0 fan status**" command on the 1RU.

Workaround: Is to issue "**show environment all**" command on the 1RU. This will provide an accurate output for current fan speed. Fan failures will be correctly defined when issuing "**show facility-alarm status**" command.

- CSCtj47086

  When a connected route that is also owned by EIGRP or OSPF is replicated from one routing table to another, any route-map that is applied after redistributing the route into EIGRP may not perform properly if the source specified during redistribution is anything other then connected (that is, EIGRP or OSPF).

  Workaround: Make sure to specify the source as EIGRP or OSPF instead of connected when redistributing the replicated routes.

- CSCtj52969

  The following message may be observed when issuing the "**show issu state detail"** command after performing an ***issu loadversion*** operation:

  ```
  %ISSU_PROCESS-3-IPC_AGENT: Failed to send; error code [ timeout ]
  ```

  This message may be observed when issuing the 'show issu state detail' command

  after performing an 'issu loadversion' operation.

  Workaround: There is no workaround.

- CSCtj55459

  No configuration seen or configuration has not taken into effect while configuring "**ip nbar protocol-discovery**" on the interfaces, only once on multiple interfaces. Except on the first interface the configuration is not seen, and on the rest of them.

  This condition may occur when the configuration is done through a script that allows for multiple interfaces to be configured in a single task and at the same time.

  Workaround: There is no workaround.

- CSCtj55916

  The ESP reloading was seen in different scenarios due to fman_fp core:

  - interface flapping
  - config/un-config interface
  - RP switchover with scalability config - 8k PVCs

  The issue could be seen in the following cases:

  - interface flapping
  - config/un-config interface
  - RP switchover with scalability config - 8k PVCs

  Workaround: The router should automatically recover after the ESP reloading.

- CSCtj57211

When exceeding the maximum session configured in a dspfarm the uSBC will reply to new call setup with SIP 500 error message, as opposed to SIP 503.

This has been observed when configuring multiple dspfarm and attempt to place more calls than defined in the maximum session parameter of a dspfarm.

Workaround: Use only one dspfarm.

- CSCtj58686

  The subclassification numbers for "**match protocol kazaa2 file-transfer**" are different for the same traffic over server port 80 and port non80.

  Workaround: There is no workaround.

- CSCtj61454

  A problem may occur when provision under codec system and is unable to be deleted.

  This problem is observed when provision under codec system is active after deletion.

  Workaround: There is no workaround.

- CSCtj64755

  Console may not activate for 4-5 mins when ima configs are removed from the virtual controller with scale.

  This condition has been observed when ima interface is configured for scale.

  Console may not activate when removing ima config from virtual controller "**no vtg 1 t1 ima-group**".

  Workaround: There is no known workaround.

- CSCtj70493

  On the Cisco ASR 1001 versions supported as of IOS XE 3.2.0S during BGP Convergence times are slower than expected.

  Note BGP Convergence does occur in all cases.

  This condition is seen during scaled configurations and becomes more apparent as BGP peer configured on the ASR1001 per peer increases.

  Workaround: There is no workaround at this time.

- CSCto03123

  Symptoms:

  1. A slow memory leak is observed on the cman_fp process on an FP and the cmcc process on a SIP. This issue is seen on all the flavors for FPs and CCs. The leak is of the order of less than 100-122K bytes per day.
  2. Additional memory leak can occur when frequent sensor value changes take place.

  Conditions: This symptom of the first leak does not occur under any specific condition. The second leak occurs when sensor-related changes take place.

  Workaround: There is no workaround.

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

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

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

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