Release 2.3 Caveats

Caveats describe unexpected behavior in Cisco IOS XE Release 2. 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 the caveats document.

This section contains open and resolved caveats for the current Cisco IOS XE maintenance release.

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

http://www.cisco.com/en/US/docs/internetworking/terms_acronyms/ita.html

This section consists of the following subsections:

Open Caveats—Cisco IOS XE Release 2.3.2

This section documents possible unexpected behavior by Cisco IOS XE Release 2.3.2

- CSCsx21652

  The **show access-list** command output does not show a packet count matching the ACL.

  Workaround: There is no known workaround.

- CSCsy16757

  When two Cisco ASR 1000 Series Routers are set up in back-to-back mode with one router configured with a static crypto map and the other with a dynamic crypto map, the router configured with the dynamic crypto map shows outbound security associations (SAs) in the pending state for unsuccessful session set-ups.

  Workaround: Ensure that configuration on both routers is correct.

  Further Problem Description: Because pending state SAs never get deleted, eventually all SAs may be used.

- CSCsy85000

  The functionality of the standby console differs based on which Route Processor (RP) is active on a Cisco ASR 1000 Series Router. If RP0 is active and RP1 is the standby, the standby console has to be enabled manually. However, if RP1 is active and RP0 is the standby, the standby console is already enabled. The functionality should be the same regardless of which RP is active and which is the standby.

  There are no known workarounds.

- CSCsy85400

  The first VIA field in a Session Initiation Protocol (SIP) INVITE/BYE call is not getting properly translated by Network Address Translation (NAT). The NAT inside IP address is replaced by some invalid characters. Calls are NOT impacted due to this issue.

This condition happens when no existing NAT translation for the session exists.

There are no known workarounds.

- CSCsy88034

  The “active” and “individual flow data” in the **show ip cache** [**verbose**] **flow** command output intermittently fails on a Cisco ASR 1000 Series Router. At times the “active” stat is zero, and at other times the individual flow data is missing.

  This problem occurs with very large configurations.

  Workaround: Reload the router.

  Further Problem Description: The management interface on a Cisco ASR 1000 Series Router cannot be used as an exporter source; this configuration is not supported.

- CSCsy31159

  When the **show history all** command is executed on a Cisco ASR 1000 Series Router, the command does not immediately reflect all commands entered.

  There are no known workarounds.

- CSCsz02478

  The virtual-access interface is not re-used after a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsz46334

  In a test run of over 41 hours—sessions and TC's are constantly churned, whereby 20% of 7.5 users perform successful acct-logon and 80% of the users receive an authorization timeout. Over the duration of this test in a session-churn scenario, a RP memory leak is observed.

  Workaround: There is no known workaround.

- CSCsz47689

  During Embedded Services Processor Stateful Switchover, it takes 1200 milliseconds before the new IPv4 VoIP call can be established. The ESP-Switchover notification takes about 1 second to reach the Standby-ESP.

- CSCsz48605

  Momentary SLOS after SSO on ATM SPA interface. Conditions are: 1) ATM OC3 SPA with interface in “link / protocol down” state. 2) SSO.

  Workaround: There is no known workaround.

  Further Problem Description: This issue happens momentarily only when interfaces are in down state and SSO is performed. SLOS will come up after that; all spurious alarms will be cleared.

- CSCsz48914

  NHRP registration and tunnels are not up between the first and second level hubs. It is observed in hierarchial topology most of the time. When Cisco ASR 1000 Series Router acts as first and second level hubs, it is observed that NHRP is flapping between them and no NHRP registration is successful. This results in DMVPN network not being up.

  Workaround: There is no known workaround.

- CSCsz49249

  Embedded Services Processor (ESP) reloads when router gets invalid (wrong) ACL attribute from RADIUS server.

Workaround: There is no known workaround.

- CSCsz54781

  On enabling interim accounting on a per-session basis, no Interim accounting updates are sent to the AAA server for PPPoX sessions.

  Workaround: There is no known workaround.

- CSCsz72070

  Upgrading QoS from Mod3 to Mod4 failed in some cases.

  Workaround: There is no known workaround.

- CSCsz82080

  Under a scaled configuration (for example, 1500 DVTI remote access sessions), when all 1500 DVTI sessions are brought up at the same time in the DVTI server, the Embedded Services Processor (ESP) may reload. The problem may occur when 1500 DVTI sessions are brought up simultaneously.

  Workaround: Bring up approximately 100 Virtual Access interfaces at one time

- CSCsz90376

  The Embedded Services Processor (ESP) on the Cisco ASR 1000 Series Router may fail after a route-map is deleted and immediately added back. This may happen when a route-map configuration used in NAT translation configuration is deleted and immediately added back.

  Workaround: Add the route-map used by NAT translation back after the previous deletion is fully completed.

- CSCta15550

  Pings to a Multicast address fail, when the Cisco ASR 1000 Series Router is configured as IPSec GETVPN group member that is registered to a Key server. Multicast traffic has to pass through the group members.

  Workaround: 1) “Shutdown” followed by “no shutdown” on the group member interface which has the gdoi crypto map. 2) Execute the **clear crypto gdoi** command.

- CSCta24676

  When an attempt is made to log in to the Kerberos client, the RP fails. After the clocks of the UUTs are synchronized and the routers are configured with kerberos credentials.

  Workaround: There are no known workarounds.

- CSCta27374

  On the ASR 1000 Series Router, the update rate for statistics given by the **show policy map** command is much greater than in prior releases. The update rate has been observed to be up to 80 seconds between updates with highly scaled configurations. Note that QoS is applied on a highly scaled configuration, for example, 16K VLANs.

  Workaround: There are no known workarounds.

- CSCta38072

  Cisco IOS XE may fail while attempting to do a “redundancy force-switchover.” This is an intermittent issue.

  During a “redundancy force switchover,” the switchover occurs, but when standby bay 0 is restarting, Cisco IOS XE fails. Cisco IOS XE in standby bay 0 then restarts and the system reaches SSO.

  Workaround: There are no known workarounds.

- CSCta40724

  The reassembly router experiences a performance degradation when QoS is applied to the far end egress interface of the fragmenting router. This issue was observed when 1500 byte traffic was sent between the two routers. Without Qos applied in the fragmenting router, the performance was 750 Mbps. With Qos applied, the performance dropped to 400 Mbps.

  Conditions: Applying Qos to the egress interface can trigger this condition on traffic that is fragmented.

  Workaround: If a priority queue can be applied on the fragmenting traffic with QoS, then the result is a performance of 700 Mbps. If no priority queue can be applied, then there is no workaround.

- CSCta50363

  This condition only occurs when a large number of pinholes, for example 1440 pinholes, subscribing to NT/QUALERT have stopped receiving traffic simultaneously. The pause only occurs after a majority of notifications have been sent through. After a 5-7 minute pause, the remaining notifications come through. In this case approximately 10-15 notifications come in late.

  Workaround: There are no known workarounds.

  Further Problem Description: This issue only occurs in the rare case that traffic is stopped on a large number of pinholes simultanesouly. The effects are not considered serious. A few pinholes may report NT/QUALERT late. The loss of synchronization for the few affected pinholes is temporary and it should not affect the availability of Cisco Unified Border Element (SP Edition) services.

- CSCta55610

  The standby processor keeps on rebooting and does not come up, after a “hw-module slot R1 reload” and ISSU downgrade. The active RP is running the prior software and the standby RP is trying to come up with the downgraded software. Error message observed is: %RF-3-NOTIF_TMO: Notification timer Expired for RF Client: Redundancy Mode RF(29)

  Workaround: There are no known workarounds.

- CSCta58849

  When reloading the router, the following error message/traceback is observed: %SCHED-7-WATCH: Attempt to set uninitialized watched boolean. This is a timing issue and should only be observed if BGP is receiving data. The impact of the traceback is minimal.

  Workaround: Performing the **no router bgp** ... command before issuing the **reload** command may avoid this traceback.

  Further Problem Description: This should have minimal impact on the router, as this is a timing issue when BGP has already shut down, but before the router has reloaded. There should be no impact to routing other than what is caused by a reload.

- CSCta61656

  The **show memory debug leaks chunks** command displays 204 bytes of extended ACL leak with basic configuration. During system initialization, there is a one time allocation of a 204 byte chunk of memory that was not freed.

  Workaround: There are no known workarounds.

- CSCta65165

  Cisco IOS XE suffers a failure while executing the **show ip ospf interface** command.

  This issue occurs under the following conditions: When the Cisco ASR 1002 Router is used as an LNS. All Virtual-Access IFs are registered as OSPF Interface. And you execute the **show ip ospf interface** command when disconnecting 1000 sessions of L2TP.

Workaround: Remove the unnumbered interface of the Virtual-Template from OSPF.

- CSCta79229

  When the route map configuration is changed on PBR configured on Virtual Template with traffic running, it may cause tracebacks on the Cisco ASR 1000 Series Router; eventually the system recovers.

  Further Problem Description: Changing the route map on the fly involves removal of route map information from the data path and addition of new route map information in the data path. Because traffic is continuously running, some lookups may fail and cause temporary error conditions.

  Workaround: There are no known workarounds.

- CSCta93930

  The Embedded Services Processor (ESP) eventually suffers a major failure after about 800,000 PPP sessions flap with the IP virtual-reassembly feature configured, either through the virtual-template or RADIUS. This problem is preceded by a %CPPDRV-4-ADRSPC_LIMIT log message.

  Conditions are: The IP virtual-reassembly feature must be configured on the virtual-template or RADIUS. PPP sessions using this feature must flap. This problem may occur on PTA sessions as well as LNS. This problem was observed on ESP20 and may occur on ESP10 as well.

  Workaround: Disable the IP virtual-reassembly feature or limit its deployment to PPP subscribers who need it. Monitor for %CPPDRV-4-ADRSPC_LIMIT log messages.

- CSCta94710

  Cisco ASR 1000 Series Route Processor (RP) fails. This problem occurs under the following conditions:

  1. You have a Cisco ASR 1000 Series Route Processor 2 (RP2).

  2. You have defined a VRF and configured it under any interface (physical/tunnel).

  3. You have disabled split horizon at interface level.

  4. You have configured EIGRP routing protocol.

  5. You advertise the network through the **address family ipv4 vrf** command.

  Workaround: Do not disable split horizon.

- CSCta99173

  The Embedded Services Processor 20 (ESP20) may core dump and reload following the churning of approximately 880,000 PPP sessions with firewall and ip virtual-reassembly features configured on those PPP sessions.

  This problem does not occur with PPP sessions that do not have VFR configured.

  This problem occurs under the following conditions: The PPP sessions must have firewall configured (have a zone configured as part of a zone-pair policy) and have ip virtual-reassembly (virtual fragmentation reassembly and VFR) configured.

  Workaround: Remove the VFR feature from the PPP sessions.

- CSCta99654

  (S,G) entry does not have the translated entry with NAT outside static/dynamic configured.

  With multicast and NAT outside static/dynamic configured, translated packets are not punted to the Route Processor (RP). The (S,G) entry on the UUT has the pre-NAT entry instead of the translated entry.

  Workaround: There is no known workaround.

Resolved Caveats—Cisco IOS XE Release 2.3.2

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.3.2.

- CSCsy05298

  When a large number of groups (for example, 50) is configured on a Cisco ASR 1000 Series Router and the **show crypto gdoi** command is issued, the IOSD process reloads.

  This condition occurs after the general configuration is applied and after the ping is checked between all the Protocol Independent Multicast (PIM) neighbors.

  Workaround: Use the **show crypto gdoi group** *group-name* command to display information for a specific group.

- CSCsy15018

  After the **show ip cache flow** command is executed 4 to 5 times on a Cisco ASR 1000 Series Router configured with NetFlow, the command returns false counters for the Total field. These false counters are only observed for a few seconds.

  This condition occurs when e**nable in/e gress netflow** is configured on 2 to 3 subinterfaces with **set term len** equal to 20.

  There are no known workarounds.

- CSCsy17832

  In rare instances, Layer 2 Tunnel Protocol (L2TP) tunnels/sessions are lost after a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsy41352

  The Cisco ASR 1000 Series Router does not generate an Internet Control Management Protocol (ICMP) redirect message over Generic Routing Encapsulation (GRE) tunnels.

  This condition occurs when there is an egress route pointing to the same GRE tunnel over which the packet came into the router.

  There are no known workarounds.

- CSCsy45907

  If the **show sbc global dbe media-stats** command is issued while the data border element (DBE) is being deleted on a Cisco ASR 1000 Series Router, the active Route Processor reloads.

  There are no known workarounds.

- CSCsy54486

  When an Internet Control Management Protocol (ICMP) Router Solicitation message is send from a source address of 0.0.0.0, the Cisco ASR 1000 Series Router drops the packet.

  There are no known workarounds.

- CSCsy58924

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reset if a certain combination of deny access control entries (ACEs) are added to a Web Cache Communication Protocol (WCCP) access control list (ACL).

  Workaround: Shut down the interface to the Wide Area Application Engine (WAE).

Further Problem Description: This problem can occur in the broadband remote access server (BRAS) scenario also and is related to the size of certain Internet Protocol Communications (IPC) messages.

- CSCsy60103

  The Cisco ASR 1000 Series Router reports a cmand crash during a router reload.

  Workaround: The router should function normally after the reload. No workaround is necessary.

- CSCsy70911

  When the source of the exporter is set to the management interface, the source displays as unknown in the output of the **show ip flow export** command.

  Workaround: Do not assign the management interface as the source of the exporter.

- CSCsy74452

  A Cisco ASR 1000 Series Router running Cisco IOS XE Release 2.3.0 cannot download an ip access-list configuration with multiple port numbers in one access control entry (ACE) to the Cisco QuantumFlow Processor.

  This error is observed if a user configures an ip access-list with more than one port number after the **eq** or **neq** keywords.

  For example:

```
Router(config)#ip access-list ext testxxx
Router(config-ext-nacl)#permit tcp any any eq 2001 2002 2003
Router(config-ext-nacl)# *Mar 28 05:34:51.576: %FMFP_ACL-3-ACL_OBJECT_DOWNLOAD: F0:
fman_fp_image: ACL actions for ACL testxxx fail to download because Bad address.
*Mar 28 05:34:51.577: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: ACL 14
download to CPP failed
```

  Workaround: Put only one port number after **eq** or **neq** keywords. The following are examples of specific workarounds:

  Example 1

  Convert one ACE configuration with multiple **eq** ports to multiple ACEs with one port as follows:

  Change the ACE from:

```
permit tcp any any eq 2001 2002 2003
```

  to:

```
permit tcp any any eq 2001
permit tcp any any eq 2002
permit tcp any any eq 2003
```

  Example 2

  Convert one ACE configuration with multiple **neq** values to multiple separate ranges as follows:

  Change the ACE from:

```
permit tcp any any neq 2001 3001
```

  to:

```
permit tcp any any lt 2001
permit tcp any any range 2002 3000
permit tcp any any gt 3001
```

Example 3

Convert one ACE configuration with multiple values for both the source and destination port to multiple combinations as follows:

Change the ACE from:

```
permit tcp any eq 2001 2002 any eq 3001 3002
```

to:

```
permit tcp any eq 2001 any eq 3001
permit tcp any eq 2001 any eq 3002
permit tcp any eq 2002 any eq 3001
permit tcp any eq 2002 any eq 3002
```

- CSCsy77269

  The Cisco ASR 1000 Series Router reloads when executing a s**how crypto ipsec sa identity** command.

  This condition seems to occur while Group Encrypted Transport VPN (GET VPN) is doing a rekey.

  Workaround: Wait for the GET VPN rekey to finish before executing a **show crypto ipsec sa identity** command. You can also increase the lifetime of the security associations (SAs) so that rekeys happen less frequently.

- CSCsy78488

  One or more of the following symptoms can be seen on a Cisco ASR 1000 Series Router:

  – The **show platform hardware cpp active feature fnf datapath all** and s**how ip cache flow** commands might not work for following aggregation caches:

    - Destination prefix aggregation (destination mask only)

    - Destination prefix TOS aggregation (destination mask only)

    - Prefix aggregation (source and destination mask)

    - Prefix-port aggregation (source and destination mask)

    - Prefix-TOS aggregation (source and destination mask)

    - Source prefix aggregation (source mask only)

    - Source prefix TOS aggregation (source mask only)

  – Denies associating the egress and ingress monitors with the caches.

  – Resource (memory) leakage

  These conditions may occur when the following configuration is configured under the **ip flow-aggregation cache** *cache-type* command sub-mode for the above mentioned cache types:

  mask {[**destination** | **source**] **minimum** *value*

  Workaround: Do not configure **mask** {[**destination** | **source**] **minimum** *value*} for the caches described in the first bullet.

  Further Problem Description: With the workaround a mask value of 0 is used as the default. As a result, NetFlow collection granularity will be coarse.

- CSCsy81461

  If a GM is left for re-keying for a long interval, NO IPSEC FLOWS messages display on the Cisco ASR 1000 Series Router console and the IPSec security association (SA) download fails.

  There are no known workarounds.

- CSCsy83163

  On a Cisco ASR 1000 Series Router, a Secure Shell (SSH) session on a Telnet connection hangs as soon as AAA Authentication is successful and the target router's prompt is received.

  Workaround: Do not attempt an SSH connection from within a Telnet session.

- CSCsy83413

  When 1k Dynamic Multipoint VPN (DMVPN) IPSec tunnels are established with a hub-spoke topology on a Cisco ASR 1000 Series Router, a memory leak occurs at the “eventutil” module.

  There are no known workarounds.

- CSCsy92358

  The IOSD process on a Cisco ASR 1000 Series Router may run out of memory if left running with an IPSec and Multipoint GRE (mGRE) configuration for long intervals.

  There are no known workarounds.

  Further Problem Description: The router may eventually reload due to an invalid handling of memory allocation failure.

- CSCsy93931

  The Cisco ASR 1000 Series Router does not reset the timeout value down to 60 seconds upon receipt of a FIN/RST/SYN for a Transmission Control Protocol (TCP) session when the **no-payload** keyword is used on the mapping. As a result, larger than expected Network Address Translation (NAT) translation tables are observed in the output of the s**how ip nat statistics** command.

  Workaround: Remove the **no-payload** keyword, or manually reset the nat tcp timeout down to 60 seconds.

- CSCsy94554

  When the **clear ipv6 neighbor** command is issued on a Cisco ASR 1000 Series Router, the adjacency of the ipv6 next-hop will be incomplete if it is needed to resolve a 6to4 tunnel.

  Workaround: Perform the **shutdown** and **no shutdown** commands on the 6to4 tunnel.

- CSCsy95109

  Some virtual circuits remain down after an asynchronous transfer mode (ATM) SPA and SIP reload.

  This condition has been observed with 100 virtual path (VP) pseudowires (PWs).

  Workaround: Enter the **clear ospf process** command.

- CSCsy96344

  When the **clear ip nat trans *** command is executed while an overloaded configuration with extremely high scaling is running, the Cisco ASR 1000 Series Router may reload.

  There are no known workarounds.

- CSCsy96501

  Performing an in-service software upgrade (ISSU) sub-package upgrade from Cisco IOS XE Release 2.2.3 to Cisco IOS XE Release 2.3.1 results in “CPPOSLIB-3-ERROR_NOTIFY” traceback and two core files while upgrading the active Embedded Services Processor (ESP).

  There are no known workarounds.

- CSCsy96761

  Removing NetFlow from the last/only interface may cause the Embedded Services Processor (ESP) on a Cisco ASR 1000 Series ESP board to reload.

This condition is caused by a race condition between the Cisco QuantumFlow Processor ager logic verses the code that processes the ager shutdown administrative action. If the ager shutdown code executes while the periodic ager function is executing, the ager function may reuse the timer structure, which is subsequently freed as part of the ager shutdown.

Workaround: The timing window can be reduced to near 0 by taking the following steps:

1. Configure NetFlow on interface x with no traffic.
2. Deconfigure NetFlow from all other interfaces.
3. Wait for all entries in the NetFlow cache to be aged out.
4. Then deconfigure NetFlow from the inactive interface x.

- CSCsy97794

  Policy Based Routing (PBR) stops working on a Cisco ASR 1000 Series Router after **ip policy route-map** is applied on the IPSec Dynamic Virtual Tunnel Interface (DVTI) interface.

  Workaround: Save the configuration and reboot the router.

- CSCsy99103

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads if a **configure replace** command is executed that results in many configuration changes.

  This condition was observed on a Cisco ASR 1004 Router running Cisco IOS XE Release 2.2.3.

  Workaround: Do use the **configure replace** command.

- CSCsz01854

  CE-to-CE communication stops after the main interface on a Cisco ASR 1000 Series Router (configured as a PE) is brought up and the Hot Standby Routing Protocol (HSRP) takes over as active on the subinterface.

  Workaround: Fail over the HSRP on the Cisco ASR 1000 Series Router to the other HSRP subinterface and then fail it back.

- CSCsz02404

  A Cisco ASR 1000 Series Router may reload when the router is configured with Network Address Translation (NAT) at extremely high dynamic bind scaling.

  There are no known workarounds.

- CSCsz04555

  A SPA-1X10GE-L-V2 on a Cisco ASR 1000 Series Router may reload when subjected to high Bit Error Rates.

  Workaround: There are no known workarounds. The module will reload and come back up. A shut/no shut should bring the interface back online.

- CSCsz05918

  Cisco Discovery Protocol (CDP) neighbors do not come up on the VLAN subinterface between two Cisco ASR 1000 Series Routers or a Cisco ASR 1000 Series Router and a Cisco 7600 Series Router or Cisco 7200 Series Router.

  This condition occurs because CDP is enabled on the VLAN subinterface but disabled on main interface.

  Workaround: Activate CDP on the main interface.

- CSCsz12276

  Dynamic Multipoint VPN (DMVPN) stops functioning if you configure a dynamic crypto map on the physical interface of a Cisco ASR 1000 Series Router running Cisco IOS XE Release 2.3.0.

  Workaround: Downgrade the software to Cisco IOS XE Release 2.2.x Cisco IOS XE Release 2.1.x.

- CSCsz18158

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may unexpectedly reload during a complex NetFlow-related reconfiguration.

  This condition is observed when a large-scale NetFlow configuration (such as many instances of NetFlow on interfaces/subinterfaces) is used in conjunction with dynamic reconfiguration. For example:

```
int range te0/2/0.2 - te0/2/0.1001
no flow-sampler abc
no flow-sampler abc eg
!
int te1/3/0
no flow-sampler abc
no flow-sampler abc eg int range te0/2/0.2 - te0/2/0.1001
flow-sampler abc
flow-sampler abc eg
!
int te1/3/0
flow-sampler abc
flow-sampler abc eg
```

  Workaround: Wait for some pending actions to complete before entering the next command.

  For example, the following command sequence shows the same sequence of commands as in the example above, but the sequence is interspersed with two wait intervals:

```
int range te0/2/0.2 - te0/2/0.1001
no flow-sampler abc
no flow-sampler abc eg
!
int te1/3/0
no flow-sampler abc
no flow-sampler abc eg
! WORKAROUND STEP
! Wait for pending actions to complete by entering the show platform soft object f0
! stat command.
! Repeat this show command until the status is "no actions pending".
int range te0/2/0.2 - te0/2/0.1001
flow-sampler abc
flow-sampler abc eg
!
int te1/3/0
flow-sampler abc
flow-sampler abc eg
! WORKAROUND STEP
! Wait for pending actions to complete by entering the show platform soft object f0
! stat command.
! Repeat this show command until the status is "no actions pending".
```

  Further Problem Description: This condition is a timing-related problem that tends to occur with a large dynamic reconfiguration. The workaround avoids the timing-related issue by enforcing atomicity between separate phases of the reconfiguration.

- CSCsz21313

  A Cisco ASR 1000 Series Router reloads with the __be_c3pl_action_account_queueing_stats_free message when removing a subscriber policy with the account feature configured from the port-channel.

  Workaround: Do not configure the account feature within a subscriber policy. The account feature is not supported in Cisco IOS XE Release 2.3.

- CSCsz21732

  A Cisco ASR 1000 Series Router may reload when configured for Simple Network Management Protocol (SNMP) inform notifications.

  Workaround: Disable inform notifications using the **no snmp-server host host-address informs** command.

- CSCsz44301

  During platform Route Processor (RP) switchover, root hub is not seeing NHRP registration messages from first level hubs. After RP swtichover, NHRP is not registered to root hub.

  Workaround: There are no known workarounds.

- CSCsz45152

  The Environment Monitoring Daemon (EMD) is a process dedicated to collection and transmission of chassis-environment statistics information such as temperature, and so forth. This process periodically transmits the information using messages.

  During the early stages of bringup (after a reload), EMD fails while attempting to create and transmit the first of one such message. This problem happens during bringup that immediately follows the router reload (using the **reload** command), with auto-boot configured. It happens in Cisco IOS XE Release 2.3.2 and earlier releases.

  Workaround: There is no workaround. EMD restarts after the failure and usually works as expected.

- CSCsz47599

  The SPA-4XT3/E3 serial interface does not come up after the router reloads. It is a timing issue and is not always seen.

  Workaround: Performing a shut and no-shut interface brings up the interface.

  Further Problem Description: Sometimes in a router reload case, if the interface state event comes earlier before the interface is registered, the event is ignored. As a workaround: perform a shut and no-shut of the interface; the system asks for another interface state event and handles bringing up the interface this time.

- CSCsz81459

  Issue 1. After Route Processor (RP) SSO on a DMVPN hub, hub locally generated packets bypass IPsec encryption on hub to spoke tunnel. The spoke will not be able process traffic generated by the hub, such as EIGRP packets. The problem is only observed when the Cisco ASR 1000 Series Router acts as a DMVPN hub and DMVPN spoke. This issue is only applicable for a Cisco ASR 1000 Series Router RP switchover.

  Workaround 1: Save the configuration and reboot the router. Preservation of IPSec sessions after SSO is not a supported feature in the release.

  Issue 2. DMVPN with IPSEC tunnel fails to come-up after SSO. This issue is DMVPN with IPSEC only and is applicable only after SSO.

  Workaround 2: Clear the adjacency.

Further Problem Description: After SSO, platform multicast adjacency is not repopulated due to race condition between tunnel-up notification and FIB repopulate request.

- CSCsz85092

  Cisco ASR 1000 Series Router fails while changing NAT configuration from Dynamic NAT to PAT with traffic on.

  Workaround: Stop the traffic and change NAT translations.

- CSCta02570

  Cisco IOS XE resets while bringing up a large number of dVTIs, in this case 1500 dVTIs, at the same time.

- CSCta04880

  This problem occurs when running EoMPLSoGREoIPSec using an IPsec protection profile on the GRE tunnel. If we unconfigure the IPsec profile from the GRE tunnel interface and it is the last IPsec tunnel configured in the router, the ESP may reload. This problem causes all traffic being forwarded by the ESP to be dropped and the Cisco ASR 1000 Series Router needs to be reloaded for services to recover.

  The problem is observed if EoMPLS over GRE tunnel traffic is being encrypted or decrypted on the Cisco ASR 1000 Series Router with ESP20 and RP1. The issue can also be seen with other types of configuration such as IPv6 IPsec SVTI configuration and EIGRP over DMVPN configuration. This problem occurs frequently under common conditions and configurations

  Workaround: Configure a dummy IPsec tunnel with no peer. Therefore, the in-use IPsec tunnel will not be the last one to be removed in the router.

- CSCta07106

  The initial packet is dropped for mcast conditions. It happens in PIM-SM and PIM-DM.

  Workaround: There is no known workaround.

- CSCta33011

  Not able to terminate PPPoE sessions on the Cisco ASR 1000 Series Router. The problem starts after days of normal working operations where the Cisco ASR 1000 Series Router is configured as an LNS.

- CSCta43602

  The MFIB code translates the packet received on the output interface to 0.0.0.0 and simply drops the packet. The PIM assert mechanism is not triggered with NAT when the original source address is the same as the translated source address.

  Workaround: There is no known workaround.

- CSCta45260

  Cisco IOS XE may fail while attempting to do IPv6 neighbor resolution. For this issue to occur, the control plane update for removing an IPv6 route must pass the in-flight request from the data-path to initiate neighbor discovery for a specific V6 address reachable by the changing route.

  Workaround: There is no known workaround.

- CSCta58499

  RP fails at the Mwheel process. This problem was observed when booting two routers at the same time or doing an RP switchover.

  Workaround: There is no known workaround.

- CSCta58589

  The cpp_cp process running on the Embedded Services Processor (ESP) fails, causing the ESP to reload. This problem is caused by a sequence of QoS configuration and interface addition/deletion changes or rate changes performed at the same time.

- CSCta58800

  An Embedded Services Processor (ESP) reset occurs and the following (or similar) error message is displayed on the system console: *Jul 8 17:53:31.674 IST: %CPPHA-3-FAULT: F0: cpp_ha: CPP:0 desc:INFP_INF_SWASSIST_LEAF_INT_INT_EVENT0 det:DRVR(interrupt) class:OTHER sev:FATAL id:1995 cppstate:RUNNING res:UNKNOWN flags:0x7 cdmflags:0x0

  This problem may occur when a hierarchical policy-map is rapidly configured, deconfigured, and configured on a GigabitEthernet interface. The parent policy-map must have serveral child classes each referencing the same output child policy-map. The child policy-map must have random-detect configured in some of its classes.

  Workaround: After deconfiguing the policy-map, wait approximately 30 seconds before reconfiguring it.

- CSCta69720

  The route processor (RP) is observed to reload after 24 hours.

  When 10K sessions out of 23K sessions are flapped for 24 hours, the RP is observed to reload and switchover is observed.

Open Caveats—Cisco IOS XE Release 2.3.1

This section documents possible unexpected behavior by Cisco IOS XE Release 2.3.1.

- CSCsy05298

  When a large number of groups (for example, 50) is configured on a Cisco ASR 1000 Series Router and the **show crypto gdoi** command is issued, the IOSD process reloads.

  This condition occurs after the general configuration is applied and after the ping is checked between all the Protocol Independent Multicast (PIM) neighbors.

  Workaround: Use the **show crypto gdoi group** *group-name* command to display information for a specific group.

- CSCsy15018

  After the **show ip cache flow** command is executed 4 to 5 times on a Cisco ASR 1000 Series Router configured with NetFlow, the command returns false counters for the Total field. These false counters are only observed for a few seconds.

  This condition occurs when **enable in/e gress netflow i**s configured on 2 to 3 subinterfaces with **set term len** equal to 20.

  There are no known workarounds.

- CSCsy16757

  When two Cisco ASR 1000 Series Routers are set up in back-to-back mode with one router configured with a static crypto map and the other with a dynamic crypto map, the router configured with the dynamic crypto map shows outbound security associations (SAs) in the pending state for unsuccessful session set-ups.

Workaround: Ensure that configuration on both routers is correct.

Further Problem Description: Because pending state SAs never get deleted, eventually all SAs may be used.

- CSCsy17832

  In rare instances, Layer 2 Tunnel Protocol (L2TP) tunnels/sessions are lost after a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsy31159

  When the **show history all** command is executed on a Cisco ASR 1000 Series Router, the command does not immediately reflect all commands entered.

  There are no known workarounds.

- CSCsy41352

  The Cisco ASR 1000 Series Router does not generate an Internet Control Management Protocol (ICMP) redirect message over Generic Routing Encapsulation (GRE) tunnels.

  This condition occurs when there is an egress route pointing to the same GRE tunnel over which the packet came into the router.

  There are no known workarounds.

- CSCsy45907

  If the **show sbc global dbe media-stats** command is issued while the data border element (DBE) is being deleted on a Cisco ASR 1000 Series Router, the active Route Processor reloads.

  There are no known workarounds.

- CSCsy54486

  When an Internet Control Management Protocol (ICMP) Router Solicitation message is send from a source address of 0.0.0.0, the Cisco ASR 1000 Series Router drops the packet.

  There are no known workarounds.

- CSCsy58924

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reset if a certain combination of deny access control entries (ACEs) are added to a Web Cache Communication Protocol (WCCP) access control list (ACL).

  Workaround: Shut down the interface to the Wide Area Application Engine (WAE).

  Further Problem Description: This problem can occur in the broadband remote access server (BRAS) scenario also and is related to the size of certain Internet Protocol Communications (IPC) messages.

- CSCsy60103

  The Cisco ASR 1000 Series Router reports a cmand crash during a router reload.

  Workaround: The router should function normally after the reload. No workaround is necessary.

- CSCsy70911

  When the source of the exporter is set to the management interface, the source displays as unknown in the output of the **show ip flow export** command.

  Workaround: Do not assign the management interface as the source of the exporter.

- CSCsy74452

  A Cisco ASR 1000 Series Router running Cisco IOS XE Release 2.3.0 can not download an ip access-list configuration with multiple port numbers in one access control entry (ACE) to the Cisco QuantumFlow Processor.

  This error is observed if a user configures an ip access-list with more than one port number after the **eq** or **neq** keywords.

  For example:

```
Router(config)#ip access-list ext testxxx
Router(config-ext-nacl)#permit tcp any any eq 2001 2002 2003
Router(config-ext-nacl)# *Mar 28 05:34:51.576: %FMFP_ACL-3-ACL_OBJECT_DOWNLOAD: F0:
fman_fp_image: ACL actions for ACL testxxx fail to download because Bad address.
*Mar 28 05:34:51.577: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: F0: fman_fp_image: ACL 14
download to CPP failed
```

  Workaround: Put only one port number after **eq** or **neq** keywords. The following are examples of specific workarounds:

  Example 1

  Convert one ACE configuration with multiple **eq** ports to multiple ACEs with one port as follows:

  Change the ACE from:

```
permit tcp any any eq 2001 2002 2003
```

  to:

```
permit tcp any any eq 2001
permit tcp any any eq 2002
permit tcp any any eq 2003
```

  Example 2

  Convert one ACE configuration with multiple **neq** values to multiple separate ranges as follows:

  Change the ACE from:

```
permit tcp any any neq 2001 3001
```

  to:

```
permit tcp any any lt 2001
permit tcp any any range 2002 3000
permit tcp any any gt 3001
```

  Example 3

  Convert one ACE configuration with multiple values for both the source and destination port to multiple combinations as follows:

  Change the ACE from:

```
permit tcp any eq 2001 2002 any eq 3001 3002
```

  to:

```
permit tcp any eq 2001 any eq 3001
permit tcp any eq 2001 any eq 3002
permit tcp any eq 2002 any eq 3001
permit tcp any eq 2002 any eq 3002
```

- CSCsy77269

  The Cisco ASR 1000 Series Router reloads when executing a s**how crypto ipsec sa identity** command.

  This condition seems to occur while Group Encrypted Transport VPN (GET VPN) is doing a rekey.

  Workaround: Wait for the GET VPN rekey to finish before executing a **show crypto ipsec sa identity** command. You can also increase the lifetime of the security associations (SAs) so that rekeys happen less frequently.

- CSCsy78488

  One or more of the following symptoms can be seen on a Cisco ASR 1000 Series Router:

  – The **show platform hardware cpp active feature fnf datapath all** and s**how ip cache flow** commands might not work for following aggregation caches:

    - Destination prefix aggregation (destination mask only)

    - Destination prefix TOS aggregation (destination mask only)

    - Prefix aggregation (source and destination mask)

    - Prefix-port aggregation (source and destination mask)

    - Prefix-TOS aggregation (source and destination mask)

    - Source prefix aggregation (source mask only)

    - Source prefix TOS aggregation (source mask only)

  – Denies associating the egress and ingress monitors with the caches.

  – Resource (memory) leakage

  These conditions may occur when the following configuration is configured under the **ip flow-aggregation cache** *cache-type* command sub-mode for the above mentioned cache types:

  mask {[**destination** | **source**] **minimum** *value*

  Workaround: Do not configure **mask** {[**destination** | **source**] **minimum** *value*} for the caches described in the first bullet.

  Further Problem Description: With the workaround a mask value of 0 is used as the default. As a result, NetFlow collection granularity will be coarse.

- CSCsy81461

  If a GM is left for re-keying for a long interval, NO IPSEC FLOWS messages display on the Cisco ASR 1000 Series Router console and the IPSec security association (SA) download fails.

  There are no known workarounds.

- CSCsy83163

  On a Cisco ASR 1000 Series Router, a Secure Shell (SSH) session on a Telnet connection hangs as soon as AAA Authentication is successful and the target router's prompt is received.

  Workaround: Do not attempt an SSH connection from within a Telnet session.

- CSCsy83413

  When 1k Dynamic Multipoint VPN (DMVPN) IPSec tunnels are established with a hub-spoke topology on a Cisco ASR 1000 Series Router, a memory leak occurs at the “eventutil” module.

  There are no known workarounds.

- CSCsy85000

  The functionality of the standby console differs based on which Route Processor (RP) is active on a Cisco ASR 1000 Series Router. If RP0 is active and RP1 is the standby, the standby console has to be enabled manually. However, if RP1 is active and RP0 is the standby, the standby console is already enabled. The functionality should be the same regardless of which RP is active and which is the standby.

  There are no known workarounds.

- CSCsy85400

  The first VIA field in a Session Initiation Protocol (SIP) INVITE/BYE call is not getting properly translated by Network Address Translation (NAT). The NAT inside IP address is replaced by some invalid characters. Calls are NOT impacted due to this issue.

  This condition happens when no existing NAT translation for the session exists.

  There are no known workarounds.

- CSCsy88034

  The “active” and “individual flow data” in the **show ip cache** [**verbose**] **flow** command output intermittently fails on a Cisco ASR 1000 Series Router. At times the “active” stat is zero, and at other times the individual flow data is missing.

  This problem occurs with very large configurations.

  Workaround: Reload the router.

  Further Problem Description: The management interface on a Cisco ASR 1000 Series Router cannot be used as an exporter source; this configuration is not supported.

- CSCsy92358

  The IOSD process on a Cisco ASR 1000 Series Router may run out of memory if left running with an IPSec and Multipoint GRE (mGRE) configuration for long intervals.

  There are no known workarounds.

  Further Problem Description: The router may eventually reload due to an invalid handling of memory allocation failure.

- CSCsy93931

  The Cisco ASR 1000 Series Router does not reset the timeout value down to 60 seconds upon receipt of a FIN/RST/SYN for a Transmission Control Protocol (TCP) session when the **no-payload** keyword is used on the mapping. As a result, larger than expected Network Address Translation (NAT) translation tables are observed in the output of the s**how ip nat statistics** command.

  Workaround: Remove the **no-payload** keyword, or manually reset the nat tcp timeout down to 60 seconds.

- CSCsy94554

  When the **clear ipv6 neighbor** command is issued on a Cisco ASR 1000 Series Router, the adjacency of the ipv6 next-hop will be incomplete if it is needed to resolve a 6to4 tunnel.

  Workaround: Perform the **shutdown** and **no shutdown** commands on the 6to4 tunnel.

- CSCsy95109

  Some virtual circuits remain down after an asynchronous transfer mode (ATM) SPA and SIP reload.

  This condition has been observed with 100 virtual path (VP) pseudowires (PWs).

  Workaround: Enter the **clear ospf process** command.

- CSCsy96344

  When the **clear ip nat trans *** command is executed while an overloaded configuration with extremely high scaling is running, the Cisco ASR 1000 Series Router may reload.

  There are no known workarounds.

- CSCsy96501

  Performing an in-service software upgrade (ISSU) sub-package upgrade from Cisco IOS XE Release 2.2.3 to Cisco IOS XE Release 2.3.1 results in "CPPOSLIB-3-ERROR_NOTIFY" traceback and two core files while upgrading the active Embedded Services Processor (ESP).

  There are no known workarounds.

- CSCsy96761

  Removing NetFlow from the last/only interface may cause the Embedded Services Processor (ESP) on a Cisco ASR 1000 Series ESP board to reload.

  This condition is caused by a race condition between the Cisco QuantumFlow Processor ager logic verses the code that processes the ager shutdown administrative action. If the ager shutdown code executes while the periodic ager function is executing, the ager function may reuse the timer structure, which is subsequently freed as part of the ager shutdown.

  Workaround: The timing window can be reduced to near 0 by taking the following steps:

  1. Configure NetFlow on interface x with no traffic.
  2. Deconfigure NetFlow from all other interfaces.
  3. Wait for all entries in the NetFlow cache to be aged out.
  4. Then deconfigure NetFlow from the inactive interface x.

- CSCsy97794

  Policy Based Routing (PBR) stops working on a Cisco ASR 1000 Series Router after **ip policy route-map** is applied on the IPSec Dynamic Virtual Tunnel Interface (DVTI) interface.

  Workaround: Save the configuration and reboot the router.

- CSCsy99103

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads if a **configure replace** command is executed that results in many configuration changes.

  This condition was observed on a Cisco ASR 1004 Router running Cisco IOS XE Release 2.2.3.

  Workaround: Do use the **configure replace** command.

- CSCsz01854

  CE-to-CE communication stops after the main interface on a Cisco ASR 1000 Series Router (configured as a PE) is brought up and the Hot Standby Routing Protocol (HSRP) takes over as active on the subinterface.

  Workaround: Fail over the HSRP on the Cisco ASR 1000 Series Router to the other HSRP subinterface and then fail it back.

- CSCsz02404

  A Cisco ASR 1000 Series Router may reload when the router is configured with Network Address Translation (NAT) at extremely high dynamic bind scaling.

  There are no known workarounds.

- CSCsz02478

  The virtual-access interface is not re-used after a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsz04555

  A SPA-1X10GE-L-V2 on a Cisco ASR 1000 Series Router may reload when subjected to high Bit Error Rates.

  Workaround: There are no known workarounds. The module will reload and come back up. A shut/no shut should bring the interface back online.

- CSCsz05918

  Cisco Discovery Protocol (CDP) neighbors do not come up on the VLAN subinterface between two Cisco ASR 1000 Series Routers or a Cisco ASR 1000 Series Router and a Cisco 7600 Series Router or Cisco 7200 Series Router.

  This condition occurs because CDP is enabled on the VLAN subinterface but disabled on main interface.

  Workaround: Activate CDP on the main interface.

- CSCsz12276

  Dynamic Multipoint VPN (DMVPN) stops functioning if you configure a dynamic crypto map on the physical interface of a Cisco ASR 1000 Series Router running Cisco IOS XE Release 2.3.0.

  Workaround: Downgrade the software to Cisco IOS XE Release 2.2.x Cisco IOS XE Release 2.1.x.

- CSCsz18158

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may unexpectedly reload during a complex NetFlow-related reconfiguration.

  This condition is observed when a large-scale NetFlow configuration (such as many instances of NetFlow on interfaces/subinterfaces) is used in conjunction with dynamic reconfiguration. For example:

```
int range te0/2/0.2 - te0/2/0.1001
no flow-sampler abc
no flow-sampler abc eg
!
int te1/3/0
no flow-sampler abc
no flow-sampler abc eg int range te0/2/0.2 - te0/2/0.1001
flow-sampler abc
flow-sampler abc eg
!
int te1/3/0
flow-sampler abc
flow-sampler abc eg
```

  Workaround: Wait for some pending actions to complete before entering the next command.

  For example, the following command sequence shows the same sequence of commands as in the example above, but the sequence is interspersed with two wait intervals:

```
int range te0/2/0.2 - te0/2/0.1001
no flow-sampler abc
no flow-sampler abc eg
!
int te1/3/0
no flow-sampler abc
```

```
no flow-sampler abc eg
! WORKAROUND STEP
! Wait for pending actions to complete by entering the show platform soft object f0
! stat command.
! Repeat this show command until the status is "no actions pending".
int range te0/2/0.2 - te0/2/0.1001
flow-sampler abc
flow-sampler abc eg
!
int te1/3/0
flow-sampler abc
flow-sampler abc eg
! WORKAROUND STEP
! Wait for pending actions to complete by entering the show platform soft object f0
! stat command.
! Repeat this show command until the status is "no actions pending".
```

Further Problem Description: This condition is a timing-related problem that tends to occur with a large dynamic reconfiguration. The workaround avoids the timing-related issue by enforcing atomicity between separate phases of the reconfiguration.

- CSCsz21313

  A Cisco ASR 1000 Series Router reloads with the __be_c3pl_action_account_queueing_stats_free message when removing a subscriber policy with the account feature configured from the port-channel.

  Workaround: Do not configure the account feature within a subscriber policy. The account feature is not supported in Cisco IOS XE Release 2.3.

- CSCsz21732

  A Cisco ASR 1000 Series Router may reload when configured for Simple Network Management Protocol (SNMP) inform notifications.

  Workaround: Disable inform notifications using the **no snmp-server host host-address informs** command.

Resolved Caveats—Cisco IOS XE Release 2.3.1

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.3.1.

- CSCsr16693

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

  Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-bundle.shtml

- CSCsr29468

  Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

- CSCsu21828

  A series of TCP packets may cause a denial of service (DoS) condition on Cisco IOS devices that are configured as Easy VPN servers with the Cisco Tunneling Control Protocol (cTCP) encapsulation feature. Cisco has released free software updates that address this vulnerability. No workarounds are available; however, the IPSec NAT traversal (NAT-T) feature can be used as an alternative.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml.

  Note: The March 25, 2009, Cisco IOS Security Advisory bundled publication includes eight Security Advisories. All of the advisories address vulnerabilities in Cisco IOS Software. Each advisory lists the releases that correct the vulnerability or vulnerabilities in the advisory. The following table lists releases that correct all Cisco IOS Software vulnerabilities that have been published in Cisco Security Advisories on March 25, 2009, or earlier.

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-bundle.shtml

- CSCsu38228

  On a Cisco ASR 1000 Series Router with Weighted Random Early Detection (WRED) enabled, when **random-detect exponential-weighting-constant** is reset with valid values (1-6, default is 4) and removed from the policy map applied, the **random-detect exponential-weighting-constant** is set to 9.

  Workaround: Reconfigure **random-detect exponential-weighting-constant** to the correct value.

- CSCsv38166

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

- CSCsv49924

  When multiple Dynamic Host Configuration Protocol (DHCP) Relay agents are present between the clients and the DHCP server, the incorrect binding and route is created on the DHCP Relay Agent.

  There are no known workarounds.

- CSCsv70092

  When executing the **redundancy force-switchover** command in a software redundant configuration on a Cisco ASR 1000 Series Router, the active Route Processor (RP) may experience a kernel driver fault and reload unexpectedly.

  There are no known workarounds; the router will recover after the RP reload.

- CSCsw46873

  When the Cisco ASR 1000 Series Router is configured as a Multicast router and packets are transmitted intermittently in an interval that is larger than the normal registry timeout period (typically, 3 minutes), the initial packet of a multicast stream may not be transmitted from source to subscribers successfully.

  This condition is observed for both Protocol Independent Multicast - Sparse Mode (PIM-SM) and Protocol Independent Multicast - Dense Mode (PIM-DM) and for both IPv4 and IPv6.

  There are no known workarounds.

- CSCsx02650

  On a Cisco ASR 1000 Series Router, malformed IPv4 fragmented packets result in reassembly failure in the virtual fragment reassembly (VFR) feature and are dropped with the following error message:

  ```
  ATTN-3-SYNC_TIMEOUT
  ```

  In addition, the Cisco QuantumFlow Processor (QFP) global drop counters indicate a reassembly failure or timeout.

  There are no known workarounds.

- CSCsx04070

  The Cisco ASR 1000 Series Router is not correctly handling double encryption with IPSec IPv4 tunnel mode.

  This condition is observed under the following configuration scenario:

  rtr_A ------ ASR1 ------ ASR2 ---- rtr_B

  where:

  - There is a transit IPSec tunnel between device A and B.
  - There is an IPSec static virtual tunnel interface (sVTI) between ASR1 and ASR2 that is supposed to encrypt the transit IPSec packets again.

  The tunnel between rtr_A and rtr_B gets established correctly, but encrypted traffic cannot be sent over the already encrypted tunnel between the routers because of double Encapsulating Security Payload (ESP) headers.

  Note that when Generic Routing Encapsulation (GRE) mode is used on the tunnel, encrypted traffic can be sent because there is a GRE header between the ESP headers.

  Workaround: Use GRE mode on the tunnel instead of IPSec IPv4 tunnel mode.

- CSCsx06021

  Auto-RP information that is received and cached on a Cisco ASR 1000 Series Router configured as the stub router of a DMVPN network is not propagated to the spoke sites.

  This condition is observed when **ip pim autorp listener** and **ip pim sparse mode** are configured throughout the network, and the Auto-RP mapping agent is configured inside the main site away from the DMVPN stub router.

  Workaround: Configure a default Protocol Independent Multicast (PIM) rendezvous point (RP) for the Auto-RP groups, and turn on the local Auto-RP group sparse mode.

- CSCsx06507

  If a Packet-over-SONET (POS) SPA experiences a loss of signal failure during a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router, a synchronization mismatch of states may occur between the SPA hardware and the RP. This intermittent condition is observed after the RP switchover if a soft or hard online insertion and removal (OIR) insertion of the SPA is performed. It may affect the functionality of higher level protocols running on the RP.

  There are no known workarounds.

  Further Problem Description: This intermittent condition is caused by a timing issue. It only occurs. when the timing of the SPA reload occurs such that events from the SPA hardware are missed.

- CSCsx10283

  Under rare conditions, the active RP2 on a Cisco ASR 1000 Series Router may reload unexpectedly when online insertion and removal (OIR) is performed on the standby RP.

  There are no known workarounds.

- CSCsx15761

  The fman-fp process on a Cisco ASR 1000 Series Router reloads.

  This condition occurs when the application of an access control list (ACL) fails as a result of Ternary Content Addressable Memory (TCAM) resource exhaustion. It may be followed by removal of the failed ACLs or disconnection of the affected sessions.

  Workaround: Prevent resource exhaustion.

- CSCsx17284

  A traffic delay of 10 seconds is observed after a Route Processor (RP) High Availability (HA) switchover on a Packet-over-SONET (POS) interface on a Cisco ASR 1000 Series Router.

  This condition occurs because when the standby RP becomes active, the POS interface is reset.

  There are no known workarounds.

- CSCsx27977

  In an IPSec network on a Cisco ASR 1000 Series Router, Border Gateway Protocol (BGP) routes may not be advertised through Generic Routing Encapsulation (GRE) tunnels.

  This condition has been observed after a Route Processor (RP) switchover or when both IPSec peers are brought up about the same time.

  Workaround: Enable **crypto ipsec frag after-encryption** in the configuration.

- CSCsx33368

  Network Address Translation (NAT) mapping using a route-map with **match interface** does not work on the Cisco ASR 1000 Series Router.

  Workaround: If possible, use **match ip nexthop** in the route-map instead.

- CSCsx39037

  The injected IPv6 or IPv4 data pak from Cisco IOS is not sent out to the Protocol Independent Multicast (PIM) tunnel on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsx51860

  In a very large Dynamic Multipoint VPN (DMVPN) network (for example, 1500 spokes connecting to a single hub), some of the tunnels may not be fully reflected in the hardware and may cause traffic drop on those tunnels.

  This condition is more likely to happen when users configure a very large number of spokes and toggle the interfaces between shut and no shut multiple times.

  Workaround: Perform **shut/no shut** on the specific spoke for which the hub does not have the entry in the hardware.

- CSCsx55431

  An Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload continuously if an online insertion and removal (OIR) insertion of ESP is performed or the ESP is reloaded while crypto session removals (**clear crypto session** commands) are being processed.

  Workaround: Before performing an ESP OIR or reload, ensure that no outstanding crypto session removals are to be processed by checking the status of the active crypto sessions on the active ESP.

- CSCsx57569

  On a Cisco ASR 1000 Series Router with hierarchical Quality of Service (QoS) applied, an unexpected reload of the Embedded Services Processor (ESP) may occur if the hierarchical policy is repeatedly removed and replaced with another policy.

  This condition occurs if the following scenario is repeated multiple times under highly scaled conditions: first the child policy is removed, then the parent policy is removed, and finally an entirely new/separate hierarchical policy is created. Note that the problem doe s not occur when only the child policy is repeatedly removed and replaced.

  Workaround: Avoid removing the child policy when wholesale QoS configuration changes are required.

- CSCsx60481

  When performing an in-service software upgrade (ISSU) upgrade to or downgrade from Cisco IOS XE Release 2.3.0, the following error messages may appear on the console:

  ```
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_sp:  cpp_sp encountered an error
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an error
  ```

  There is no service impact due to these error messages, and the upgrade/downgrade completes successfully.

  There are no known workarounds.

- CSCsx61701

  The Cisco ASR 1000 Series Router may reload after the Network Address Translation (NAT) High Speed Logger (HSL) is unconfigured and later re-configured.

  Workaround: When you unconfigure NAT high speed logging (v9), reload the router to prevent the risk of potential problems.

- CSCsx62253

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads when a configuration change is made to the Firewall High Speed Logger (HSL).

  This condition may occur when HSL is removed using the **no log flow-export v9 udp destination** command and then re-configured using the **log flow-export v9 udp destination** command.

  Workaround: Do not remove the HSL configuration unless all of the Firewall configuration is to be removed. You can modify the HSL configuration.

- CSCsx63557

  When Layer 2 Tunnel Protocol (L2TP) sessions are created and then torn down by Intelligent Services Gateway (ISG), the Cisco QuantumFlow Processor (QFP) leaks DRAM memory.

  There are no known workarounds.

- CSCsx63585

  On a Cisco ASR 1000 Series Router, the repeated set-up and teardown of large numbers of Intelligent Services Gateway (ISG) sessions over the Layer 2 Tunnel Protocol (L2TP) results in a memory leak on the Embedded Services Processor (ESP). The leak is small, and no service impact is expected under normal operating conditions.

  There are no known workarounds.

- CSCsx63860

  When you perform an in-service software upgrade (ISSU) downgrade to Cisco IOS XE Release 2.3.0 on a Cisco ASR 1000 Series Router containing an operational SPA-4XOC3-POS-V2 SPA, the following messages appear on the active RP console:

  ```
  %IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex for an  interface on the
  Standby, allocating a new ifindex from the Active (ifindex=58, idbtype=SWIDB)
  ```

  Workaround: Shut down the SPA-4XOC3-POS-V2 SPA before beginning the downgrade process and then bring the SPA back up after the downgrade is complete.

- CSCsx67820

  When a firewall is configured on a Cisco ASR 1000 Series Router and the **no debug platform hardware qfp active feature firewall datapath global all detail** command is issued, a lot of messages may flood the console.

  Workaround: Avoid using the **no debug platform hardware qfp active feature firewall datapath global all detail** command.

- CSCsx68791

  The following traceback is observed on the console of a Cisco ASR 1000 Series Router when a class map is removed and added from a crypto interface:

  ```
  *Feb 12 21:23:45.134: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:033
  TS:00000021156554985833 %QOS-3-INVALID_CLASS_QID: Class Queuing error for interface
  TenGigabitEthernet1/3/0.4002, qid 9293 vqid 0 -Traceback= 802437f8 8009fd39 82003612
  8036b9bb 801f6f00 820126ac 80020064 80020055
  *Feb 12 21:23:45.134: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:033
  TS:00000021156555178393 %QOS-3-VALID_DEFAULT_QID: Using Default Queue for interface
  TenGigabitEthernet1/3/0.4002, qid 63 vqid 63 -Traceback= 802437f8 8009fdcd 82003612
  8036b9bb 801f6f00 820126ac 80020064 80020055   ent-6ru-2(config-pmap-c)#end
  ```

This message is not observed with regular interfaces.

Workaround: This traceback is transient and harmless. To avoid the traceback when policy map changes are required, perform the following steps: remove the policy map from the interface, make the changes to it, and then reapply the policy map.

- CSCsx71752

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload due to a cpp_cp process failure when using a non-existent ACE ID value in the **show platform hardware qfp active feature ipsec spd** *spdId* **ace** *aceId cgId* command to check IPSec counters.

  Workaround: Use the appropriate ACE ID value returned by the IPSec platform commands.

- CSCsx76396

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when a crypto map is removed from the configuration and the crypto map contains a match for a clear text packet. For example:

```
crypto dynamic-map dyn_map 10
set ip access-group 102 in
set ip access-group 103 out
set transform-set t1
crypto map testmap 10 ipsec-isakmp dynamic dyn_map

interface GigabitEthernet0/0/1
ip address 16.0.0.1 255.255.255
ip access-group 104 in
ip access-group 105 out
no ip unreachables
negotiation auto
crypto map testmap
```

  There are no known workarounds.

- CSCsx76862

  On a Cisco ASR 1000 Series Router with the Virtual Fragmentation and Reassembly (VFR) feature enabled, the VFR processing of fragments can get stuck, and all fragments requiring VFR processing are dropped. There is no impact on any traffic not requiring VFR processing.

  There are no known workarounds.

- CSCsx77598

  If the **show platform hardware cpp active feature qos police output interface** *interface-name* command is executed during an in-service software upgrade (ISSU) from Cisco IOS XE Release 2.2 to Cisco IOS XE Release 2.3 on a Cisco ASR 1004 or Cisco ASR 1002 router, the following error message may occur:

```
% Error: QOS transaction processing in progress, try again later
```

  This condition is observed when the router is configured with Quality of Service (QoS) and the command is executed after the Route Processor (RP) is upgraded to Cisco IOS XE Release 2.3 but while the Embedded Services Processor (ESP) is still running the Cisco IOS XE Release 2.2.

  Workaround: Do not issue the **show** command in the middle of the ISSU procedure.

- CSCsx79872

  Under rare conditions, after Network Address Translation (NAT) is completely unconfigured (and not re-configured), a reload of the Cisco ASR 1000 Series Router may occur.

  Workaround: Remove NAT before reloading the router.

- CSCsx80170

  On a Cisco ASR 1000 Series Router configured with the Multicast Source Discovery Protocol (MSDP), a Reverse Path Forwarding (RPF) check on a multicast packet may fail and the multicast traffic will not be forwarded.

  There are no known workarounds.

- CSCsx83387

  When performing a downgrade to Cisco IOS XE Release 2.3.0, the standby Cisco IOS process, which is still running Cisco IOS XE Release 2.3.0, fails to start and prevents the downgrade from completing.

  There are no known workarounds.

- CSCsy01886

  On a Cisco ASR 1000 Series Router with an RP2, PPP over Ethernet (PPPoE) subscribers whose sessions terminate at an L2TP Network Server (LNS) fail to authenticate if they have a RADIUS-supplied user profile with an attribute of the type "**lcp:interface-config=**...".
  A Cisco ASR 1000 Series Router with an RP1 is not affected.

  This condition is observed under the following scenario:

  - The "**lcp:interface-config=**... " attribute in a RADIUS user profile is used to configure features on a session. For example, "**lcp:interface-config=zone-member security DoS-max-zone**" is used with a firewall configuration, or "**lcp:interface-config=ip vrf forwarding vrf1**" is used with a VRF forwarding configuration.
  - The zone member for the PPPoE subscriber is downloaded using RADIUS.

  Workaround: Define PPPoE subscriber features in virtual templates.

- CSCsz80074

  Due to a minor change in the build script for Cisco IOS XE Release 2.3.0 and Cisco IOS XE Release 2.3.1, the Cisco IOS XE Release 2.3.0 and Cisco IOS XE Release 2.3.1 images can be 15 to 30 MB larger than intended.

  Workaround: If the image size of Cisco IOS XE Release 2.3.0 or Cisco IOS XE Release 2.3.1 is not causing any issues, no action is necessary, however, these images will no longer be downloadable on Cisco.com. Replacement images (Cisco IOS XE Release 2.3.0t and Cisco IOS XE Release 2.3.1t) with exactly the same content and bug fixes will be available on Cisco.com. Old image MD5 sums will still be available for verification on the download page.

Open Caveats—Cisco IOS XE Release 2.3.0

This section documents possible unexpected behavior by Cisco IOS XE Release 2.3.0.

- CSCsu38228

  On a Cisco ASR 1000 Series Router with Weighted Random Early Detection (WRED) enabled, when **random-detect exponential-weighting-constant** is reset with valid values (1-6, default is 4) and removed from the policy map applied, the **random-detect exponential-weighting-constant** is set to 9.

  Workaround: Reconfigure **random-detect exponential-weighting-constant** to the correct value.

- CSCsu52126

  When the **redundancy force-switchover** command is executed from slot 0 to slot 1 on a Cisco ASR 1000 Series Router, the recovery time is several seconds more than when the switchover is done in reverse (from slot 1 to slot 0).

  There is no failure on the switchover, only a delay in the time that the router starts forwarding legacy traffic to or receiving traffic from the new IOSd instance.

  There are no known workarounds.

- CSCsu80584

  During an in-service software upgrade (ISSU) downgrade to the Cisco IOS XE Release 2.3 or Cisco IOS XE Release 2.2 image on a Cisco ASR 1000 Series Router, the following traceback is observed:

  ```
  %FMANRP_OBJID-5-DUPCREATE: Duplicate forwarding object creation obj_handle
  ```

  There are no known workarounds.

- CSCsv49924

  When multiple Dynamic Host Configuration Protocol (DHCP) Relay agents are present between the clients and the DHCP server, the incorrect binding and route is created on the DHCP Relay Agent.

  There are no known workarounds.

- CSCsx06021

  Auto-RP information that is received and cached on a Cisco ASR 1000 Series Router configured as the stub router of a DMVPN network is not propagated to the spoke sites.

  This condition is observed when **ip pim autorp listener** and **ip pim sparse mode** are configured throughout the network, and the Auto-RP mapping agent is configured inside the main site away from the DMVPN stub router.

  Workaround: Configure a default Protocol Independent Multicast (PIM) rendezvous point (RP) for the Auto-RP groups, and turn on the local Auto-RP group sparse mode.

- CSCsv69275

  If a Cisco ASR 1000 Series Router cannot successfully perform IPv6 neighbor-discovery, it does not send an ICMP unreachable packet to the originator of the packet.

  There is no known workaround other than configuring static Neighbor Discovery (ND) entries.

- CSCsv70092

  When executing the **redundancy force-switchover** command in a software redundant configuration on a Cisco ASR 1000 Series Router, the active Route Processor (RP) may experience a kernel driver fault and reload unexpectedly.

  There are no known workarounds; the router will recover after the RP reload.

- CSCsv99477

  The following REASSEMBLY_ERR message appears on the IOS console on a Cisco ASR 1000 Series Router:

  ```
  frag info reference counter reaches  zero
  ```

  This condition occurs when Network Address Translation (NAT) is enabled, fragments are received out-of-order, and the Cisco QuantumFlow Processor (QFP) has to drop the packets because it cannot put them in order for NAT. These fragmented packets are most likely dropped.

  There are no known workarounds.

- CSCsw23314

  The Cisco ASR 1000 Series Router reloads when a manual keyed crypto map is removed from an interface after unconfiguring the tunnel source.

  This condition occurs when the user cuts and pastes several "**no**" forms of CLI commands to delete the tunnel source interface, the crypto map from the tunnel, and the tunnel interface itself.

  For example:

```
conf t
int tunnel0
no ip addr x.x.x.x x.x.x.x
no tunnel source e1/0
no tunnel dest y.y.y.y
no crypto map ! must be a manual keyed crypto map
exit
no interface tunnel0
```

  Workaround: Enter the commands one at a time, and wait after removing the tunnel source. This workaround will prevent the race condition from occurring and avoid the reload.

- CSCsw29132

  A group member may not receive retransmit rekeys if any of the following conditions occur:

  - An access control list (ACL) is added to the key server.
  - An ACL is changed on the key server.
  - The retransmit CLI parameter is changed on the key server.

  There are no known workarounds.

- CSCsw39916

  When you remove an IPv4 or IPv6 address from a Session Border Controller (SBC) interface, either directly or indirectly by removing virtual routing and forwarding (VRF) forwarding or VRF definitions, the media addresses or media pools that are configured on the SBC interface remain configured even though these addresses refer to IP addresses that were deleted.

  Possible affected commands include the following:

  no ip address *address mask*

  no ip address

  no ipv6 address *address-specification*

  no ipv6 address

  no vrf forwarding

  no VRF definition *vrf-name*

  Workaround: Remove the media addresses or media pools from the SBC interface before removing or causing the removal of IP addresses on the SBC interface.

  Further Problem Description: Leaving media addresses or media pools configured on an SBC interface after their IP addresses have been removed from the SBC interface may cause routing problems for future calls. If an IP address that was removed is associated with a non-default VRF, then adding back the VRF does not solve the problem. You must unconfigure the SBC interface.

- CSCsw41261

  Under very rare conditions, an RP2 on a Cisco ASR 1000 Series Router may reload during its initial boot because of a missing bootflash device. The following messages are observed on the console:

  ```
  %IOSXEBOOT-4-DEVICE_MISSING: (rp/0): Integrity check for missing device /dev/bootflash
  not performed.  %IOSXEBOOT-1-BOOTFLASH_FAILED_MISSING: (rp/0): Required Bootflash disk
  failed or missing, reloading system
  ```

  These messages are followed by a reload of the RP2. The subsequent reload is successful and the condition appears to clear.

  There are no known workarounds; the system self-recovers.

- CSCsw45701

  Under very rare conditions, an RP2 on a Cisco ASR 1000 Series Router may experience an unexpected reload during intensive file-system operations to the USB-based file systems (bootflash:, usb0:/usb1:).

  Workaround: Limit the USB file-system operations. For example, avoid copying to and from bootflash and to and from external USB sticks.

- CSCsw46873

  When the Cisco ASR 1000 Series Router is configured as a Multicast router and packets are transmitted intermittently in an interval that is larger than the normal registry timeout period (typically, 3 minutes), the initial packet of a multicast stream may not be transmitted from source to subscribers successfully.

  This condition is observed for both Protocol Independent Multicast - Sparse Mode (PIM-SM) and Protocol Independent Multicast - Dense Mode (PIM-DM) and for both IPv4 and IPv6.

  There are no known workarounds.

- CSCsw47239

  A Cisco ASR 1006 Router with an RP2 configured with Route Processor Redundancy (RPR) experiences traffic loss exceeding the expected threshold of 100 seconds on an RP switchover. This issue is not observed with an RP1.

  There are no known workarounds.

  Further Problem Description: In RPR mode, after an RP switchover, the Embedded Services Processors (ESPs) and SIPs are reset. Both the ESPs and the SPAs (which are present in the SIPs) take more than 100 seconds to boot up. During this interval, traffic loss is experienced.

- CSCsw66319

  The following traceback message may be observed on a Cisco ASR 1000 Series Router when you bring up a large number of PPP over Ethernet (PPPoE) sessions with a Quality of Service (QoS) policy applied to them at a high rate of session setup:

  ```
  %QOS-3-INVALID_CLASS_QID
  ```

  There are no known workarounds.

- CSCsw81617

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may unexpectedly restart during a reconfiguration.

  This condition is observed when certain combinations of features are configured concurrently on the same interface, such as the combination of NetFlow and Unicast Reverse Path Forwarding (uRPF).

Workaround: Performing the following steps may help mitigate this issue:

1. Execute a **shut** at the interface.
2. Remove features from the interface.
3. Re-add the desired features to the interface.
4. Execute **no shut** at the interface.

- CSCsw88573

  A process on the standby Route Processor (RP) on a Cisco ASR 1000 Series Router may reload during an in-service software upgrade (ISSU) downgrade from Cisco IOS XE Release 2.3.0 to Cisco IOS XE Release 2.2.2. This condition may also delay new IPSec tunnel establishment. If the process has already been reloaded three times since the IOSd process came online, the IOSd process may also reload.

  This condition occurs when the second RP is to be installed with Cisco IOS XE 2.2.0 software packages after the first RP switchover during the ISSU downgrade process.

  Workaround: If IPSec is deployed, bring down the IPSec tunnels before downgrading from Cisco IOS XE Release 2.3.0.

- CSCsw96044

  The Cisco IOS process on a Cisco ASR 1000 Series Router may reset when virtual routing and forwarding (VRF) forwarding is enabled on a T3 Frame-Relay subinterface after IP address configuration on the interface.

  There are no known workarounds.

- CSCsx01992

  Upgrading the ROMmon image on an RP2 in a Cisco ASR1006 Router may fail when the RP2 is the active RP and in slot 1.

  Workaround: Perform the ROMmon upgrade in slot 0 only, and swap boards to complete the upgrade for both RPs.

- CSCsx02650

  On a Cisco ASR 1000 Series Router, malformed IPv4 fragmented packets result in reassembly failure in the virtual fragment reassembly (VFR) feature and are dropped with the following error message:

  ```
  ATTN-3-SYNC_TIMEOUT
  ```

  In addition, the Cisco QuantumFlow Processor (QFP) global drop counters indicate a reassembly failure or timeout.

  There are no known workarounds.

- CSCsx05516

  The Cisco ASR 1000 Series Router may drop packets with an IP format error if the key server is configured with time based anti-replay and an Embedded Services Processor (ESP) switchover is triggered on the chassis.

  Workaround: Initiate a re-key after every ESP switchover.

- CSCsx06507

  If a Packet-over-SONET (POS) SPA experiences a loss of signal failure during a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router, a synchronization mismatch of states may occur between the SPA hardware and the RP. This intermittent condition is observed after the RP switchover if a soft or hard online insertion and removal (OIR) insertion of the SPA is performed. It may affect the functionality of higher level protocols running on the RP.

  There are no known workarounds.

  Further Problem Description: This intermittent condition is caused by a timing issue. It only occurs. when the timing of the SPA reload occurs such that events from the SPA hardware are missed.

- CSCsx10283

  Under rare conditions, the active RP2 on a Cisco ASR 1000 Series Router may reload unexpectedly when online insertion and removal (OIR) is performed on the standby RP.

  There are no known workarounds.

- CSCsx13031

  The Route Processor (RP) on a Cisco ASR 1000 Series Router may reload unexpectedly shortly after switchover.

  This condition is observed when the **redundancy force-switchover** command is executed immediately (within seconds) after the system reaches Stateful Switchover (SSO) mode.

  There are no known workarounds.

- CSCsx15761

  The fman-fp process on a Cisco ASR 1000 Series Router reloads.

  This condition occurs when the application of an access control list (ACL) fails as a result of Ternary Content Addressable Memory (TCAM) resource exhaustion. It may be followed by removal of the failed ACLs or disconnection of the affected sessions.

  Workaround: Prevent resource exhaustion.

- CSCsx15768

  The active Route Processor (RP) on a Cisco ASR 1000 Series Router reloads and a core dump is generated when encapsulation is changed from **encapsulation frame-relay** to **no encapsulation frame-relay** on a serial interface.

  This condition occurs under the following scenario:

  – The Cisco ASR 1000 Series Router has **ipv6 multicast-routing** enabled.

  – The router has at least one serial interface configured with **encapsulation frame-relay**.

  – That particular serial interface has both IPv4 and IPv6 addresses configured.

  – The frame-relay encapsulation is removed by executing the **no encapsulation frame-relay** command on the serial interface.

  Workaround: There are two workarounds for this problem:

  1. Remove the IPv6 configuration by executing the **no ipv6 enable** and **no ipv6 address** commands on the serial interface, perform the encapsulation change, and then re-configure the IPv6 configuration.
  2. Shut down the serial interface, remove the frame-relay encapsulation, and then execute **no shutdown** on the interface.

- CSCsx17284

  A traffic delay of 10 seconds is observed after a Route Processor (RP) High Availability (HA) switchover on a Packet-over-SONET (POS) interface on a Cisco ASR 1000 Series Router.

  This condition occurs because when the standby RP becomes active, the POS interface is reset.

  There are no known workarounds.

- CSCsx18983

  When a Quality of Service (QoS) parent policy with 256 class maps is applied and removed from an interface on a Cisco ASR 1000 Series Router, the CPPOSLIB-3-ERROR_NOTIFY error message is generated and traceback is observed on the console. There is no service impact due to this error message.

  There are no known workarounds.

- CSCsx26324

  If an RP2 ROMmon upgrade on the Cisco ASR 1000 Series Router fails to boot the newly installed ROMmon, the router continues to attempt to boot using the failed ROMmon.

  This condition occurs only if the newly installed ROMmon cannot successfully initialize itself and reach the ROMmon prompt.

  Workaround: When the router returns to the ROMmon prompt after exhausting the maximum number of boot attempts, the upgrade pending setting can be cleared manually from the ROMmon CLI by executing the **priv**, **clrdip**, and **reset** commands in sequence. After executing these commands, the router should be able to boot using the previously installed ROMmon.

- CSCsx27977

  In an IPSec network on a Cisco ASR 1000 Series Router, Border Gateway Protocol (BGP) routes may not be advertised through Generic Routing Encapsulation (GRE) tunnels.

  This condition has been observed after a Route Processor (RP) switchover or when both IPSec peers are brought up about the same time.

  Workaround: Enable **crypto ipsec frag after-encryption** in the configuration.

- CSCsx30747

  During an in-service software upgrade (ISSU) from Cisco IOS XE Release 2.2.2 to Cisco IOS XE Release 2.3.0 on a Cisco ASR 1000 Series Router, the following error message may be generated:

  ```
  %FMANRP_OBJID-5-DUPCREATE
  ```

  This condition may occur because of a race condition on the serial subinterfaces between Frame-Relay encapsulation and configuring/unconfiguring IPv4 andIPv6 addresses.

  There are no known workarounds.

- CSCsx33368

  Network Address Translation (NAT) mapping using a route-map with **match interface** does not work on the Cisco ASR 1000 Series Router.

  Workaround: If possible, use **match ip nexthop** in the route-map instead.

- CSCsx35419

  On a Cisco ASR 1000 Series Router, the Enhanced Interior Gateway Routing Protocol (EIGRP) may flap on Dynamic Multipoint VPN (DMVPN) tunnels with tunnel protection configured.

  This condition may occur when the EIGRP control traffic has a packet size that is greater than the tunnel interface maximum transmission unit (MTU) and tunnel protection is configured.

  Workaround: Do not use tunnel protection when the EIGRP packet size can be greater than the tunnel interface MTU.

- CSCsx39037

  The injected IPv6 or IPv4 data pak from Cisco IOS is not sent out to the Protocol Independent Multicast (PIM) tunnel on a Cisco ASR 1000 Series Router.

  There are no known workarounds.

- CSCsx46099

  Under rare conditions, when there is a Cisco QuantumFlow Processor (QFP) fault and subsequent core dump on a Cisco ASR 1000 Series Router, the affected Embedded Services Processor (ESP) may experience a secondary kernel fault during the shutdown/reload of the ESP. This condition increases the time for the ESP to reload up to 10 minutes.

  There are no known workarounds. The affected ESP will restart normally after the kernel fault generates a core dump.

- CSCsx47529

  Under rare conditions, a defective hard disk drive may cause the RP2 on a Cisco ASR 1000 Series Router to hang indefinitely during startup.

  Workaround: Remove the defective hard disk from the RP2 and power cycle the RP2. The RP2 should start successfully with reduced functionality (no persistent logging or core dump collection). Request a return materials authorization (RMA) for the defective hard disk drive.

- CSCsx48566

  When the same child policy is used by two hierarchical parent policies that have different output in a broadband Quality of Service (QoS) configuration on a Cisco ASR 1000 Series Router, and the Change of Authorization (CoA) tool is used to change the session output qos hierarchical policy, the CPPOSLIB-3-ERROR_NOTIFY message appears on the console.

  Workaround: Define individual child polices for each of the parent policies.

- CSCsx51265

  When a Route Processor (RP) on a Cisco ASR 1000 Series Router is reloaded with a Quality of Service (QoS) policy that has 256 class maps contained in the policy and this policy is applied to a crypto interface, traceback is observed at cpp_bqs_mgr_lib.

  There are no known workarounds.

- CSCsx51860

  In a very large Dynamic Multipoint VPN (DMVPN) network (for example, 1500 spokes connecting to a single hub), some of the tunnels may not be fully reflected in the hardware and may cause traffic drop on those tunnels.

  This condition is more likely to happen when users configure a very large number of spokes and toggle the interfaces between shut and no shut multiple times.

  Workaround: Perform **shut/no shut** on the specific spoke for which the hub does not have the entry in the hardware.

- CSCsx55431

  An Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload continuously if an online insertion and removal (OIR) insertion of ESP is performed or the ESP is reloaded while crypto session removals (**clear crypto session** commands) are being processed.

  Workaround: Before performing an ESP OIR or reload, ensure that no outstanding crypto session removals are to be processed by checking the status of the active crypto sessions on the active ESP.

- CSCsx57569

  On a Cisco ASR 1000 Series Router with hierarchical Quality of Service (QoS) applied, an unexpected reload of the Embedded Services Processor (ESP) may occur if the hierarchical policy is repeatedly removed and replaced with another policy.

  This condition occurs if the following scenario is repeated multiple times under highly scaled conditions: first the child policy is removed, then the parent policy is removed, and finally an entirely new/separate hierarchical policy is created. Note that the problem doe s not occur when only the child policy is repeatedly removed and replaced.

  Workaround: Avoid removing the child policy when wholesale QoS configuration changes are required.

- CSCsx57787

  In a large IPSec configuration (such as 1K Generic Routing Encapsulation (GRE) tunnels) on a Cisco ASR 1000 Series Router, the standby Embedded Services Processor (ESP) may reload during a Route Processor (RP) switchover.

  This condition may occur when **tunnel protection ipsec profile** is configured on the GRE tunnel interfaces in scaled configurations of 1K GRE tunnels. The standby ESP may reload after the RP switchover if the switchover is initiated by the active RP on slot 1.

  There are no known workarounds.

- CSCsx58136

  The following message may appear during a Route Processor (RP) switchover on a Cisco ASR 1000 Series Router:

  ```
  %PMAN-3-PROCHOLDDOWN: F0: pman.sh: The process fman_fp_image has been helddown
  ```

  This condition can occur when a router with dual RPs is configured with Stateful Switchover (SSO) and a Quality of Service (QoS) policy.

  There are no known workarounds.

- CSCsx60175

  When IPv6 multicast packets are sent through IPv6-over-IPv4 tunnels on a Cisco ASR 1000 Series Router, the IPv6 packets are sent as register packets, not as native packets.

  There are no known workarounds.

- CSCsx60481

  When performing an in-service software upgrade (ISSU) upgrade to or downgrade from Cisco IOS XE Release 2.3.0, the following error messages may appear on the console:

  ```
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_sp:  cpp_sp encountered an error
  %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an error
  ```

  There is no service impact due to these error messages, and the upgrade/downgrade completes successfully.

  There are no known workarounds.

- CSCsx61692

  The Cisco ASR 1000 Series Router does not respond with a valid Router Advertisement and IPv6 prefix when the packet receives an ALL-ROUTER-MULTICAST address packet.

  There are no known workarounds.

- CSCsx61701

  The Cisco ASR 1000 Series Router may reload after the Network Address Translation (NAT) High Speed Logger (HSL) is unconfigured and later re-configured.

  Workaround: When you unconfigure NAT high speed logging (v9), reload the router to prevent the risk of potential problems.

- CSCsx62253

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads when a configuration change is made to the Firewall High Speed Logger (HSL).

  This condition may occur when HSL is removed using the **no log flow-export v9 udp destination** command and then re-configured using the **log flow-export v9 udp destination** command.

  Workaround: Do not remove the HSL configuration unless all of the Firewall configuration is to be removed. You can modify the HSL configuration.

- CSCsx62653

  When in-service software upgrade (ISSU) is performed, ISSU-related objects in the CISCO-RF-MIB return null strings.

  Workaround: Use the **show issu state detail** command instead.

- CSCsx63557

  When Layer 2 Tunnel Protocol (L2TP) sessions are created and then torn down by Intelligent Services Gateway (ISG), the Cisco QuantumFlow Processor (QFP) leaks DRAM memory.

  There are no known workarounds.

- CSCsx63585

  On a Cisco ASR 1000 Series Router, the repeated set-up and teardown of large numbers of Intelligent Services Gateway (ISG) sessions over the Layer 2 Tunnel Protocol (L2TP) results in a memory leak on the Embedded Services Processor (ESP). The leak is small, and no service impact is expected under normal operating conditions.

  There are no known workarounds.

- CSCsx63860

  When you perform an in-service software upgrade (ISSU) downgrade to Cisco IOS XE Release 2.3.0 on a Cisco ASR 1000 Series Router containing an operational SPA-4XOC3-POS-V2 SPA, the following messages appear on the active RP console:

  ```
  %IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex for an  interface on the
  Standby, allocating a new ifindex from the Active (ifindex=58, idbtype=SWIDB)
  ```

  Workaround: Shut down the SPA-4XOC3-POS-V2 SPA before beginning the downgrade process and then bring the SPA back up after the downgrade is complete.

- CSCsx64518

  Using jumbo frames (greater than 18000 bytes) on the management Ethernet port of the RP2 on a Cisco ASR 1000 Series Router may cause the resulting frames to be dropped and the following buffer error to be generated:

  ```
  %SYS-2-INPUT_GETBUF: Bad getbuffer, bytes= 18030, for interface= GigabitEthernet0
  ```

  Workaround: Reduce the size of frames on the management Ethernet network to less than 18K in size.

- CSCsx67122

  The console baud rate of an RP2 on a Cisco ASR 1000 Series Router does not function properly when set to speeds other than default value of 9600 baud.

  This condition is observed when the console baud rate is changed either in the ROMmon or in the Cisco IOS configuration.

  Workaround: Do not configure baud rates other than default value of 9600 baud on the console.

- CSCsx67820

  When a firewall is configured on a Cisco ASR 1000 Series Router and the **no debug platform hardware qfp active feature firewall datapath global all detail** command is issued, a lot of messages may flood the console.

  Workaround: Avoid using the **no debug platform hardware qfp active feature firewall datapath global all detail** command.

- CSCsx68133

  The output of the **show policy-map type inspect zone-pair** *zone-pair-name* **session** command on a Cisco ASR 1000 Series Router displays some packet counts without protocol names.

  This condition is observed when a firewall is configured, a class map is being modified while in use, the policy is attached to a zone-pair, and the class map is experiencing high traffic.

  Workaround: Execute the **clear zone-pair** *zone-pair-name* **counter** command to clear the irregular counters.

- CSCsx68348

  When the **loadversion** command is issued for an RP package (on slot 0), the changed software fails to start.

  This condition is intermittent.

  There are no known workarounds.

- CSCsx68791

  The following traceback is observed on the console of a Cisco ASR 1000 Series Router when a class map is removed and added from a crypto interface:

  ```
  *Feb 12 21:23:45.134: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:033
  TS:00000021156554985833 %QOS-3-INVALID_CLASS_QID: Class Queuing error for interface
  TenGigabitEthernet1/3/0.4002, qid 9293 vqid 0 -Traceback= 802437f8 8009fd39 82003612
  8036b9bb 801f6f00 820126ac 80020064 80020055
  *Feb 12 21:23:45.134: %IOSXE-3-PLATFORM: F0: cpp_cp: QFP:00 Thread:033
  TS:00000021156555178393 %QOS-3-VALID_DEFAULT_QID: Using Default Queue for interface
  TenGigabitEthernet1/3/0.4002, qid 63 vqid 63 -Traceback= 802437f8 8009fdcd 82003612
  8036b9bb 801f6f00 820126ac 80020064 80020055   ent-6ru-2(config-pmap-c)#end
  ```

This message is not observed with regular interfaces.

Workaround: This traceback is transient and harmless. To avoid the traceback when policy map changes are required, perform the following steps: remove the policy map from the interface, make the changes to it, and then reapply the policy map.

- CSCsx68821

  On a Cisco Systems ASR 1000 Series Router with hierarchical Quality of Service (QoS) applied, an unexpected reload of the Embedded Services Processor (ESP) may occur if the hierarchical policy is removed and re-attached.

  This condition occurs when hierarchical QoS is applied on a subinterface that has multiple Generic Routing Encapsulation (GRE) tunnels.

  Workaround: Avoid removing and re-attaching a hierarchical policy map on a subinterface with multiple GRE tunnels.

- CSCsx71472

  Interface names may be improperly filtered on a Cisco ASR 1000 Series Router running NetFlow. This condition can cause interfaces to appear to have flows that really do not exist and are actually present on a different interface. For example, flows may appear to be present on interfaces that do not have NetFlow configured.

  This condition can be observed by executing the **show ip cache** *interface* **flow** command. This issue does not impact exported flows; it only impacts flows shown on the router console.

  There are no known workarounds. This bug is cosmetic.

- CSCsx71660

  When the **test platform hardware slot r1 oir power-cycle** command is executed on a Cisco ASR 1000 Series Router, the Route Processor (RP) goes into the disabled state.

  There are no known workarounds.

- CSCsx71752

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload due to a cpp_cp process failure when using a non-existent ACE ID value in the **show platform hardware qfp active feature ipsec spd** *spdId* **ace** *aceId cgId* command to check IPSec counters.

  Workaround: Use the appropriate ACE ID value returned by the IPSec platform commands.

- CSCsx73902

  When match protocols are removed from an already applied policy-map (class_zone_1) on a Cisco ASR 1000 Series Router, sessions are not cleared even after clearing the sessions multiple times. The expectation is that after the class-map matching protocols are removed, the traffic should pass through the class-default. Even after clearing the sessions, some sessions are still established in the class-map (class_zone_1).

  This condition is observed when Zone-Based Firewall has High Availability (HA) enabled (that is, the standby Embedded Services Processor (ESP) is enabled). When HA is disabled (that is, the standby ESP is in the disabled state), the condition is not observed.

  Workaround: Reload the ESPs.

- CSCsx76396

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when a crypto map is removed from the configuration and the crypto map contains a match for a clear text packet. For example:

```
crypto dynamic-map dyn_map 10
set ip access-group 102 in
set ip access-group 103 out
set transform-set t1
crypto map testmap 10 ipsec-isakmp dynamic dyn_map

interface GigabitEthernet0/0/1
ip address 16.0.0.1 255.255.255
ip access-group 104 in
ip access-group 105 out
no ip unreachables
negotiation auto
crypto map testmap
```

  There are no known workarounds.

- CSCsx76862

  On a Cisco ASR 1000 Series Router with the Virtual Fragmentation and Reassembly (VFR) feature enabled, the VFR processing of fragments can get stuck, and all fragments requiring VFR processing are dropped. There is no impact on any traffic not requiring VFR processing.

  There are no known workarounds.

- CSCsx77598

  If the **show platform hardware cpp active feature qos police output interface** *interface-name* command is executed during an in-service software upgrade (ISSU) from Cisco IOS XE Release 2.2 to Cisco IOS XE Release 2.3 on a Cisco ASR 1004 or Cisco ASR 1002 router, the following error message may occur:

```
% Error: QOS transaction processing in progress, try again later
```

  This condition is observed when the router is configured with Quality of Service (QoS) and the command is executed after the Route Processor (RP) is upgraded to Cisco IOS XE Release 2.3 but while the Embedded Services Processor (ESP) is still running the Cisco IOS XE Release 2.2.

  Workaround: Do not issue the **show** command in the middle of the ISSU procedure.

- CSCsx78315

  If tunnel mode is changed from **gre multipoint** to **gre ip** while traffic is passing though the tunnel interface on a Cisco ASR 1000 Series Router, the IOSd process may reset.

  There are no known workarounds.

- CSCsx79872

  Under rare conditions, after Network Address Translation (NAT) is completely unconfigured (and not re-configured), a reload of the Cisco ASR 1000 Series Router may occur.

  Workaround: Remove NAT before reloading the router.

- CSCsx80170

  On a Cisco ASR 1000 Series Router configured with the Multicast Source Discovery Protocol (MSDP), a Reverse Path Forwarding (RPF) check on a multicast packet may fail and the multicast traffic will not be forwarded.

  There are no known workarounds.

- CSCsx83387

  When performing a downgrade to Cisco IOS XE Release 2.3.0, the standby Cisco IOS process, which is still running Cisco IOS XE Release 2.3.0, fails to start and prevents the downgrade from completing.

  There are no known workarounds.

- CSCsy01886

  On a Cisco ASR 1000 Series Router with an RP2, PPP over Ethernet (PPPoE) subscribers whose sessions terminate at an L2TP Network Server (LNS) fail to authenticate if they have a RADIUS-supplied user profile with an attribute of the type "**lcp:interface-config=**...".
  A Cisco ASR 1000 Series Router with an RP1 is not affected.

  This condition is observed under the following scenario:

  – The "**lcp:interface-config=**... " attribute in a RADIUS user profile is used to configure features on a session. For example, "**lcp:interface-config=zone-member security DoS-max-zone**" is used with a firewall configuration, or "**lcp:interface-config=ip vrf forwarding vrf1**" is used with a VRF forwarding configuration.

  – The zone member for the PPPoE subscriber is downloaded using RADIUS.

  Workaround: Define PPPoE subscriber features in virtual templates.