Release 2.4 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 2.4.4

This section documents possible unexpected behavior by Cisco IOS XE Release 2.4.4.

- CSCsv66827

  When clearing the SSH sessions from a VTY session causes the ASR 1000 Router Series to crash.

  Workaround:There is no workaround.

- 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.

- CSCsz01980

  The RP1 may experience unexpected watchdog timeout and reload.

  Under very rare conditions, an RP1 may experience a watchdog timeout during boot or shutdown and subsequently generate a kernel core dump.

  Workaround: No known workaround; following reload, the RP works as expected.

- CSCsz21624

  When doing **no router ospf** a message similar to the following may be seen:

```
%IPRT-3-NDB_STATE_ERROR: NDB state error (BAD EVENT STATE) (0x0) 10.10.10.3/32, state
7, event 0->4, nh_type 1 flags 4 -Process= "OSPF-1 Router", ipl= 0, pid= 268
```

The following conditions have been observed:

1. When there are significant number of IGP routes.
2. An interface has OSPF configured on a Cisco ASR 1000 Router, while running and comes up, when cleanup of the OSPF process is in progress.

Workaround: Is to remove any **network** statements in OSPF before removing the OSPF instance.

- CSCsz47878

  When provisioning LI tap with the same session ID when Radius has been configured on a Cisco ASR 1000 Router, there is a chance that traceback is observed.

  This condition has been observed when an invalid provision of LI tap is used. A unique session ID should be used for each session provisiioning.

  Workaround: Is to use a unique session ID for each session to be provisioned.

- CSCsz62927

  Sometimes header-compression commands may disappear from the configuration after reload has happened on a Cisco ASR 1000 Router.

  This condition has been seen when the following commands seems to be disappear after reload:

  ip rtp header-compression ip tcp header-compression

  Workaround: None

- CSCsz83305

  L2TP tunnel resync duration on a Cisco ASR 1000 Router is observed to be significantly longer an RP2 Route Processor compared to an RP1 Route Processor. For example, around 90 seconds on an RP2 vs 30 seconds on an RP1 for the same number of tunnels (12 000).

  This condition has been observed when the scaling numbers reached over 24k sessions and 12k tunnels.

  Workaround: None

- CSCta31582

  The netflow export command **ip flow-export version 9 bgp-nexthop** by itself has no effect meaning no BGP nexthop information is placed into the Netflow cache or records as a result of the bgp-nexthop token. If instead the commmands **ip flow-export version 9 origin-as bgp-nexthop** or **ip flow-export version 9 origin-as** are issued, then BGP nexthop information is included in all cases.

  This can occur on any Cisco ASR 1000 Router when running the NetFlow feature.

  Workaround: The workaround is covered in the above description. If BGP Nexthop info is desired configure either <*origin-as*> or <*peer-as*> in the exporter command and this will cause BGP Nexthop information to appear in the cache and the export records.

- CSCta35043

  There are numerous amount of chunk leaks observed when using **tcl scripting** commands on a Cisco ASR 1000 Router. This condition has been seen when configuring and unconfiguring the **tcl scripting** related commands, numerous chunk leaks are observed.

  Workaround: None

- CSCta37670

The ASR 1000 Router crash as a longer interrupt hold, when a single MPLS scales up to 300K prefixes.

This instance occurs only when a single MPLS with 300K prefixes. The issue does not occur with 100 prefixes.

Workaround: Is not to run 300 prefixes.

- CSCtb13902

  Password encryption with **key config-key** command on one end of tunnel results in IPSec session to fail.

  This condition has been with a back to back router running IPSec6.

  Workaround: None

- CSCtb30072

  With a 1K DMVPN spoke, if you un/re-configure tunnel protection several times and un/re-configure tunnel interface may reset both Embedded Services Processors (ESPs).

  Workaround: After unconfiguring a tunnel interface with 1K DMVPN spoke, wait for a few seconds before reconfiguring the same tunnel interface with same DMVPN configuration.

- CSCtb37274

  If billing is enabled with a valid cache path as part of the SBC configuration, and records are being written to a removable device, such as a USB drive, and the device is removed from the router, an unexpected system reload can occur.

  This issue occurs if billing records are being written to a removable device and while operations are active, the device is removed from the router. Upon replacing the device and attempting to deactivate billing, an unexpected system reload occurs.

  Workaround: To avoid this issue, do not remove the device billing records are cached to while records are being processed.

- CSCtb49373

  When static route is pointing to next-hop (without exiting an interface)this does NOT get removed from the routing table when route towards next-hop disappears on the ASR 1000 Router Series.

  This condition may occur when there is a less specific static route including the prefix of the static route are not removed.

  Workaround: Is to specify an exit interface in addition of next-hop.

- CSCtc45832

  When tracking stops the data-plane logs out of the PKT-MEM trace log this problem will occur on the ASR 1000 Router Series the sessions will be dropped and the QoS hierarchy will shut down. There also will be pending queue objects waiting to be flushed out in the list.

  The following command will show the BQS RM status:

  show plat hard qfp act inf bqs stat

  In rare conditions, an error may occur for extreme over-subscribed enviroments. When sending 10G (For example: 5G as priority, and 5G as non-priority) traffic to a 1G interface.

  All priority and control packets are dropped by the hardware this occur when the packet buffers are depleted; and when the schedule stops forwarding output packets

  Workaround: There is no known workaround to this problem.

- CSCtd58836

When changing DMVPN tunnel source this may result in having hung sessions on a Cisco ASR 1000 Router.

This condition has been seen when the Cisco ASR 1000 Router Series is running IOS XE 2.4 and up to 12.2(33)XND2.

Workaround: Is to shutdown the tunnel interfaces before changing their physical source interfaces.

- CSCtd75807

  OSPF route convergence may be slow when a large number of prefixes are to be downloaded to the ESP.

  This condition may only occur when using RP1 and ESP-10 blades.

  Workaround: There is no workaround.

- CSCte81385

  When show network-clock indicates a “valid” BITS clock state as “valid but not present” on the ASR 1000 Router Series. When a “valid” state BITS clock is removed and re-added, then show network-clock indicates BITS state as “valid but not present” even though the Active Source indicates as BITS.

  Workaround: There is no workaround. This seems to be a display issue with the show network-clock cli output due to the fact that BITS is indicated as the Active Source.

- CSCte83888

  When PoD request contains target Acct-Session-Id prepended with NAS-Port-ID

  it will not be honored.

  This condition has been observed, when PoD prepended is configured with NAS-Port-Id for target sessions.

  Workaround: Is to use only the Session-Id which is located after the, “_” in the Account-Session-ID

  to specify the session needing disconnect.

- CSCte82240

  SBC accepts “.” when key_addr_type is “DIALED_DIGITS”. This condition can occur, when set exact matching means has been set as:

  rpsRtgActionKeyAddrWildcardType to AMB_MW_EXPLICIT_WILDCARD.

  This is possible to have a “.” when rpsRtgActionKeyAddrType is set to AMB_MW_ADDR_TYPE_DIALED_DIGITS. However, it is no longer allowed when rpsRtgActionKeyAddrWildcardType is AMB_MW_EXPLICIT_WCARD (which means SBC should perform an explicit match).

  Workaround: None

- CSCte97907

  On a Cisco ASR 1000 Router with RP2 may get out of sync with NTP master every 18 minutes for approximately 1 minute. This may offset the NTP Master which will cause an increase up to -1052.1 msec and the sync will get lost.

  This instance has been observed, when NTP is enabled and running apr. 20 minutes.

  Workaround: None

Resolved Caveats—Cisco IOS XE Release 2.4.4

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.4.4

- CSCsw67249

  When a Cisco ASR 1000 Router is acting as a relay, a request for an IP address from a DHCP client fails when the DHCP client is set to unicast.

  This symptom is observed when DHCP clients and the DHCP server are in the same VRF and the DHCP clients are set to unicast.

  Workaround: If the DHCP clients allow it use broadcast method.

  Workaround: There is no workaround.

- CSCsx66105

  Chunk memory leaks at **SADB SA Header** are seen on a Group Domain of Interpretation (GDOI) group member.

  This symptom is observed when IPsec security associations (SAs) are cleared using the command **clear crypto gdoi**.

  Workaround: There is no workaround.

- CSCsy23839

  On Cisco ASR 1000 Router Series, CPU utilization of SIP (SPA Interface Processor) may be 100%.

  This symptom is observed with the following procedure:

  1. Open a terminal window for telnet to ASR 1000.
  2. Telnet to ASR 1000.
  3. Run the request platform software console attach x/x (login SIP IOS) command.
  4. Close the terminal window without exiting from SIP IOS.
  5. You can see that the ioscon process is not terminated and its CPU utilization is around 100% by the monitor platform software process command.

  Workaround: Resetting the SIP resolves the issue.

- CSCsz83570

  SSH sessions disconnect during large data exchanges, such as large logs with pagers.

  The symptom is observed when large amounts of data are exchanged between both ends: client and server (i.e.: the client provides a large input to the server and the server has a large output to send to the client). The session gets hung momentarily and disconnects after the timeout period of 120 seconds.

  Workaround: Use 3DES for encryption.

- CSCta23902

  On a DMVPN router, when the IPSec SAs are deleted, the NHRP holdtime is set to be 5 seconds. This 5 seconds gap between IPSec and the corresponding NHRP cache entry could cause the spoke to spoke tunnel to bounce under certain timing conditions.

  This symptom only occurs under certain timing conditions.

  Workaround: There is no workaround.

- CSCta46347

Connecting a 2 or 4 port OC48 POS SPA{SPA-2XOC48-POS/RPR or SPA-4XOC48-POS/RPR} back to back with either 1, 2 or 4 port OC48 POS SPA{SPA-2XOC48-POS/RPR or SPA-4XOC48-POS/RPR or SPA-1XOC48-POS/RPR} could push the corresponding POS inteface into down/down with SLOS.

This symptom is a timing related issue and could be triggered with the following sequence of operations:

1. Insert the 2 or 4 port OC48 SPA{SPA-2XOC48-POS/RPR or SPA-4XOC48-POS/RPR} without any cable connected.
2. Connect the cables.
3. Do 'no shut' (enable) on the ports.

This could result in the POS interfaces being stuck in SLOS.

Workaround: Enable (do no shut) the ports before fiber is connected.

- CSCtb79600

  IPSec tunnel does not come back up after issuing the **clear crypto session** command at the hub.

  This symptom is observed when bringing up a 2547oDMVPN (RFC 2547) network with one hub and one spoke, and the **clear crypto session** command is issued at the hub.

  Workaround: Issue the **clear crypto session** command at the spoke.

- CSCtc14197

  The following Traceback is seen on the router console following which FP reloads:

```
*Sep 23 09:37:04.432 UTC: %CPPOSLIB-3-ERROR_NOTIFY: F0: cpp_cp:  cpp_cp encountered an
error -Traceback= 1#3c307  1031ab84e4601e29a1edaf6b55a   errmsg:D976000 1C00
cpp_common_os:E0C6000 B7C0 cpp_common_os:E0C6000 18B78 cpp_exmem_mgr:ED34000 894C
cpp_wccp_svr_lib:F5DB000 E508 cpp_wccp_svr_lib:F5DB000 107AC cpp_wccp_svr_lib:F5DB000
ACB0 cpp_wccp_svr_lib:F5DB000 7368 cpp_common_os:E0C6000 10618 cpp_common_os:E0C6000
1097C evlib:DD2D000 DBA4 evlib:DD  2D000 FED4 cpp_common_os:E0C6000 11F18 :10000000
3DD0 c:BE2D200 1D078
This symptom is observed when WCCP is un-configured in a specific fashion:
ip wccp 61
ip wccp 62
interface gigabitEthernet 1/3/2
       ip wccp 61 redirect in
       ip wccp 62 redirect in
no ip wccp 62
no ip wccp 61
interface gigabitEthernet 1/3/2
      no  ip wccp 61 redirect in
      no ip wccp 62 redirect in
```

  Workaround: Un-configure WCCP by removing the service applied on the interface first and then removing the global wccp configuration:

```
interface gigabitEthernet 1/3/2
      no  ip wccp 61 redirect in
      no ip wccp 62 redirect in
no ip wccp 61
no ip wccp 62
```

- CSCtc24940

  Tracebacks are seen when crypto profile is applied when L2TP sessions are being brought up.

  This symptom is observed when a crypto profile is not defined and applied to vpdn-group while sessions are being brought up.

Workaround: There is no workaround.

- CSCtc61038

  Tracebacks are seen after removing and adding the Web Cache Communication Protocol (WCCP) service.

  This symptom is observed while traffic is flowing through the router.

  Workaround: There is no workaround.

- CSCtc79484

  Statistics for max-entries limit are not shown.

  This symptom is observed for ASRNAT under all conditions.

  Workaround: There is no workaround.

- CSCtc87430

  The following errors are seen on Active RP during RP switchover with scaled sessions (around 5k):

  asr1000 bsess: RPC header processing failed, error=5001.

  This symptom is observed when the setup is:

  Agilent---(atm)---MCP----(10GB)-----LNS(c10k)-----Agilent

  and the steps followed are:

  1. Configure MCP as LAC with Model D2.1 QOS
  2. Start session bring-up
  3. At aroung 5k session, issue RP swo4. Noticed errors on new Active RP

  Workaround: There is no workaround.

- CSCtc91560

  High CPU utilization occurs.

  The symptom is observed with session churn.

  Workaround: There is no workaround.

- CSCtd00489

  A traceback indicating that the object was being deleted before the ideal exponent is invalidated is logged.

  This symptom is observed while an ATM VC schedule is being deleted. A schedule object is freed before its ideal exponent is invalidated. This condition is treated as an error because it points to a missing step in cleaning up prior to destroying an object since it could potentially impact the rate accuracy in the future.

  Workaround: There is no workaround.

- CSCtd05011

  A buffer overflow can occur which does not have a known impact on router behavior, but may result in a potential memory access violation.

  This symptom occurs when the random number generator function is triggered.

  Workaround: There is no workaround.

- CSCtd21590

  RP crashes after executing no import ipv4 unicast map filter command.

This symptom is observed when BGP import events debugging is on with debug ip bgp import updates or debug ip bgp import event.

Workaround: Do not enable debug ip bgp import event or debug ip bgp import update.

- CSCtd22064

  An ASR 1000 Router Series will crash when removing SBC configuration after a failover.

  During normal call operations a failover is initiated via CLI. Normal call operations continue without issue after the failover. After stopping all calls, the SBC configuration is removed and the ASR 1000 will crash.

  Workaround: Do not remove SBC configuration.

- CSCtd25664

  1. ERSPAN session are not sending traffic to the analyser.
  2. ERSPAN session are not filtering traffic as expected on the router.

  This condition has been observed, when the Cisco ASR 1000 Router is running 12.2(33)XND1 and previous versions.

  1. ERSPAN configured with vlan filtering
  2. ERSPAN configured with vlan sourcing

  Workaround:

  1. Filter traffic on the analyser.
  2. There is no known workaround.

- CSCtd38347

  CPP can run out of memory and cause FPs to reload.

  This symptom is observed when flapping LNS firewall sessions are running over time on the router.

  Workaround: There is no workaround.

- CSCtd61194

  When configuring ERSPAN on FastEthernet, gives an error:

  SPAN is not supported on SPA interface

  ```
  ASR1K(config-mon-erspan-src)#source interface ?FastEthernet FastEthernet IEEE
  802.3GigabitEthernet GigabitEthernet IEEE 802.3z Port-channel Ethernet Channel of
  interfaces TenGigabitEthernet  Ten Gigabit Ethernet
  ASR1K(config-mon-erspan-src)#source interface fastEthernet 0/3/0 SPAN is not supported
  on SPA interface (FastEthernet0/3/0)ASR1K(config-mon-erspan-src)#
  ```

  This symptom is observed on Cisco ASR 1000 Router Series running Version 2.4.1 of Cisco IOS XE.

  Workaround: Configure ERSPAN on GigabitEthernet.

- CSCtd68955

  FMAN-FP may crash with netflow configuration.

  This symptom is observed on ASR1000 Router Series with enabled 2k interfaces, with full and sampled netflow in both ingress and egress direction, and router boot up with netflow configuration.

  Workaround: There is no workaround.

- CSCtd72416

  An error message with a traceback is observed on the router console in the format:

```
%FRAG-3-REASSEMBLY_DBG: Reassembly/VFR encountered an error: VFR failed at refrag:,
first fragment length 370, non-first frag total length 608.
```

The length values may change depending on the actual fragmented packets received by the router.

This symptom is observed when the IP Virtual Reassembly (VFR) feature is enabled on the interface that receives malformed fragmented packets. VFR drops such problem packets as they cannot be correctly processed and generates the error message as a warning.

Workaround: Disable the source of the malformed fragments or disable VFR feature. There is no other workaround.

- CSCtd72441

  On a Cisco ASR 1000 Router Series, when the command **show platform software wccp <*service-id*> counters** is executed, the obj_id field in the output in rare situations may be a large negative number. This is a cosmetic issue and does not affect functionality.

  This symptom is observed when:

  1. WCCPv2 is configured on the router and is redirecting traffic.
  2. The object id value is greater that 2147483647.
  3. The command **show platform software wccp <*service-id*> counters** is executed.

  Workaround: There is no workaround.

- CSCtd75033

  Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability.

  Note Note: The fix for this vulnerability has a behavior change affect on Cisco IOS Operations for Mode 7 packets. See the section Further Description of this release note enclosure.

  Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

  ntp master <*any following commands*>

  ntp peer <*any following commands*>

  ntp server <*any following commands*>

  ntp broadcast client

  ntp multicast client

  The following example identifies a Cisco device that is configured with NTP:

  ```
  router#show running-config | include ntp
  ntp peer 192.168.0.12
  ```

  The following example identifies a Cisco device that is not configured with NTP:

  ```
  router#show running-config | include ntp
  router#
  ```

  To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the show version command to display the system banner. The system banner confirms that the

  device is running Cisco IOS Software by displaying text similar to “Cisco Internetwork Operating System Software” or “Cisco IOS Software.” The image name displays in parentheses, followed by “Version” and the Cisco IOS Software

release name. Other Cisco devices do not have the show version command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
 Cisco Internetwork Operating System Software
 IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
 Technical Support: http://www.cisco.com/techsupport
 Copyright ) 1986-2008 by cisco Systems, Inc.
 Compiled Mon 17-Mar-08 14:39 by dchih
 <output truncated>
```

The following example shows a product that is running Cisco IOS Software

release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
<output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link:

http://www.cisco.com/warp/public/620/1.html

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Note Note: NTP peer authentication is not a workaround and is still a vulnerable configuration.

*** NTP Access Group**

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```
!--- Configure trusted peers for allowed access
access-list 1 permit 171.70.173.55
!--- Apply ACE to the NTP configuration
ntp access-group peer 1
```

For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

*** Infrastructure Access Control Lists**

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
!---
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
 INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Note: If the router is acting as a NTP broadcast client
!---   via the interface command "ntp broadcast client"
!---   then broadcast and directed broadcasts must be
!---   filtered as well.  The following example covers
!---   an infrastructure address space of 192.168.0.X
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 255.255.255.255 eq ntp
!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the mutlicast group must
!---   be filtered as well.  The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 239.0.0.1 eq ntp
!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.
access-list 150 deny udp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations.  Permit all other traffic to transit the
!--- device.
access-list 150 permit ip any any
!--- Apply access-list to all interfaces (only one example
!--- shown)
interface fastEthernet 2/0
 ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control List" presents guidelines and recommended deployment techniquesfor infrastructure protection access lists and is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

*** Control Plane Policing**

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, whilst the second looks at rate limiting NTP traffic to the box.

– Filtering untrusted sources to the device.

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Feature: Network Time Protocol (NTP)
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 123
!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.
access-list 150 permit udp any any eq 123
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all drop-udp-class
 match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
policy-map drop-udp-traffic
 class drop-udp-class
 drop
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
control-plane
service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action (not shown) are not affected by the policy-map drop function.

– Rate Limiting the traffic to the device

The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning **Warning: If the rate-limits are exceeded valid NTP traffic may also bedropped.**

```
!--- Feature: Network Time Protocol (NTP)
access-list 150 permit udp any any eq 123
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all rate-udp-class
match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
```

```
!--- for more information on choosing the most
!--- appropriate traffic rates
policy-map rate-udp-traffic
class rate-udp-class
police 10000 1500 1500 conform-action transmit
exceed-action drop violate-action drop
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
control-plane
 service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

Further Description: Cisco IOS Software releases that have the fix for this Cisco bug ID, have a

behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID, will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message:

Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command <cmd>ntp allow mode private</cmd> should be configured. This is disabled by default.

This is the same as the vulnerability which is described in:

http://www.kb.cert.org/vuls/id/568372

Cisco has release a public facing vulnerability alert at the following link:

http://tools.cisco.com/security/center/viewAlert.x?alertId=19540

Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

All other versions of Cisco IOS and Cisco IOS XE Software are affected.

To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returnseither of the following commands listed then the device is vulnerable:

- CSCtd83822

  Increasing memory usage of **reflector.sh** and **droputil.sh** process.

  Workaround: There is no workaround.

- CSCte05713

  The command **sh crypto map gdoi fail-close** has incorrect output.

  Workaround: There is no workaround."

- CSCte08145

  CPP reset after sending malformed GRQ.

  This symptom is observed where an ASR 1000 Router Series is performing ALG. The CPP will reset after some time period.

  Workaround: There is no workaround.

- CSCte38945

  Unable to get ping reply from the multicast group configured on loopback interface.

  The symptom can occur when there are multiple routes populated in an interface and the interface goes down. All the routers associated with the interface should be removed, but only one is deleted. This results in the ping failure.

  Workaround: Shut down the other interfaces associated with the router and enable it again.

- CSCte43708

  QFP crash on ASR 1000 Router Series.

  This symptom is observed when QFP is forwarding an IP fragment while doing IP virtual-reassembly, which is enabled by NAT.

  Workaround: There is no workaround.

- CSCte50144

  Router reports incorrect CPU utilisation. It reports a low CPU utilisation and also reports an overall utilisation lower then the utilisation under interrupts.

  For example:

  ```
  CPU utilization for five seconds: 5%/25%; one minute: 8%; five minutes: 8%
  ```

  This symptom is observed on an ASR1002 router under high CPU utilisation of the RP CPU, caused by excessive rate of punted traffic.

  Workaround: There is no workaround.

- CSCte50721

  During stateful NAT sync of H323 information from primary to standby, standby crashes.

  This symptom is observed on an ASR 1000 Router Series with dual RP and ESP.

  Workaround: Disable H323 with the following commands if H323 ALG is not required:

  no ip nat service h225

  no ip nat service ras

- CSCte51959

  QFP validates the ICMP checksum of all ICMP packets received to a local address even when we ping with 'validate reply data=no'.

  Workaround: There is no workaround.

- CSCte56627

  1. Sessions may not be synchronized properly to standby.

  OR

  2. Session deletes may not be synchronized properly to standby (session that should be deleted on standby, will not be deleted).

  Symptom 1 is observed on ASRNAT when there is an inside mapping and outside static mapping configuration.

  Symptom 2 is observed when a very high burst of session aging occurs.

  Workaround: There is no workaround.

- CSCte57362

FP reset on sending h323 V5 calls via ASR 1000 Router where ASR 1000 is configured with the NAT.

V5 h323 calls should go through ASR-NAT.

Workaround: There is no workaround.

- CSCte60069

  During the scale testing with ModelF applied on PTA, reparenting operation results in FP crash. Also CPUHOG and TIMEHOG tracebacks observed.

  This symptom is observed after the following steps:

  1. PTA: Bring up 24K IPv4 sessions, 2PQ+2CQ(modelf)
  2. Remove grandparent shaper
  3. Add the shaper back.

  Workaround: Avoiding reparenting with large number of vlans/sessions."

- CSCte64646

  A ucode interrupt occurs which causes a driver lockdown.

  This symptom is observed with QoS applied and traffic flowing, when random-detect AND fair-queue are configured in any class, and random-detect is removed from the class (on-the-fly).

  Workaround: If the problem occurs, the FP/ESP must be rebooted. To avoid the problem, stop all traffic or remove the QoS policy from the interface first, then modify that class, then re-apply QoS or restart the traffic.

- CSCte69621

  Missing CLI for configuring deny policy options. “crypto ipsec ipv4-deny {clear|deny|jump}”

  Workaround: There is no workaround."

- CSCte72128

  After a reload, “cdp enable” is missing on previously configured interfaces.

  This symptom is observed on ASR 1000 Router Series running 12.2(33)XNE1, with “cdp enable” configured on some interfaces prior to a reload. After the reload the running-config shows “cdp enable” missing on the previously configured interfaces.

  Workaround: After a reload, manually reconfigure cdp enable."

- CSCte72288

  After changing source VLAN on the source ERSPAN session to a non-existant VLAN or native VLAN (1), traffic is still being received on the SPAN port.

  This symptom is observed on ASR 1000 Router Series with VLANS on a 1Gig port as well as FE port.

  Workaround: There is no workaround."

- CSCte77136

  CLNS routing over GRE tunnels is not working on the ASR 1000 Router.

  This symptom is observed on ASR 1000 Router Series where CLNS routing over GRE tunnels is configured with a GRE tunnel as the egress interface (output from the ASR1000). In this scenario, CLNS packets are not forwarded via fast switching.

  Workaround: Use the following configuration change (needed on a per interface basis):

  “no clns route-cache” to **disable** CLNS fast switching.

- CSCte77167

  Memory leak is observed in QFP, ESP. ESP is also observed to reload after 30hrs of flapping IPv6 sessions

  This symptom is observed on ASR 1000 Router Series with IPv6 session flaps on LNS.

  Workaround: There is no workaround.

- CSCte78589

  FP reload may occur. Crash decode may look like this:

  BackTrace

```
#0  abort () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/logger.c:683
#1  0x8022f779 in rbuf_ooh_handler () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/hardware/cpp/hal/hal_dtl.c:2973
#2  0x800207f0 in _GeneralException () at
/auto/edatools/tensilica/RB-2008.4-linux/cpp/xtensa-elf/src/handlers/exc-prehandler.S:
340
#3  0x8002bc2a in cpp_reuse_req_q_insert () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/hardware/cpp/hal/hal_dtl.c:971
#4  0x802250f4 in cpp_reuse () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/cpp_reuse.c:324
#5  0x801dc3fa in chunk_free () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/chunk.c:1514
#6  0x8004d000 in ipv4_nat_free_all_seq_delta_nl () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_alg_
api.c:1219
#7  0x8004d0e1 in ipv4_nat_remove_appl_data () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_alg_
api.c:1385
#8  0x801b7eb1 in ipv4_nat_destroy_session () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_db.c
:832
#9  0x801ab07c in ipv4_nat_unlock_session () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_db.c
:1301
#10 0x801a66cc in ipv4_nat_sess_timeout () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_db.c
:1560
#11 0x801a6ce5 in ipv4_nat_sess_age () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_db.c
:1890
#12 0x801a6de0 in ipv4_nat_sess_age_to () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/dplane/feature/nat/ipv4_nat_time
.c:189
#13 0x80252ee4 in time_process_timer_ev () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/time.c:717
#14 0x802555e4 in process_recycle_control () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/control_rx.c:95
#15 0x80257c1e in mpass_restart_processing () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/multipass.c:1233
#16 0x820128dd in main () at
/auto/mcpbuilds3/release/02.05.01/BLD-02.05.01/cpp/dp/infra/packet.c:282
```

  This symptom occurs rarely but it is more likely to occur with long-lived TCP connections.

  Workaround: A possible workaround is to lower the **ip nat trans tcp-timeout** <***n***>'value.

- CSCte84990

  In a deployment with IPsec SVTI to MPLS, down stream traffic from MPLS core is not label switching. However this might be just a broken counter because there is no traffic drop.

This symptom is observed on ASR 1000 Router Series when the "sh mpls forwarding" command is run. The Bytes Label Switched counter displays 0.

Workaround: There is no workaround.

- CSCte91369

  The following show commands will give a command line error:

  sh ip cache [prefix mask] verbose flow

  sh ip cache [prefix mask] verbose flow aggregation [aggregation name]

  This symptom is observed after the following steps:

  1. Enable netflow on ASR1000 Router using the command **ip flow ingress|egress** on any interface.
  2. Send traffic through this interface.
  3. Execute the command **show ip cache flow**. The flow entries should be displayed.
  4. Try to execute the show command to filter the flows using prefix:

     sh ip cache [prefix mask] verbose flow or

     sh ip cache [prefix mask] verbose flow aggregation [agg name]

  These commands will give a parsing error.

  Workaround: Run the same commands without **verbose** option.

  The command **show ip cache flow**, which will display all entries, will work.

- CSCte93229

  An ESP crash is observed.

  This symptom is observed on an ASR 1000 Router Series with a fragmented datagram whose size exceeds 9k and DF is set.

  Workaround: There is no workaround.

- CSCte94156

  ASR 1000 running Release 2.5.1 fails to update the PST value in TBAR, causing other GM to fail sending traffic via the ASR with anti-replay error messages. This happens wherever the local ACL is changed on the GM or by KS failure and recovery.

  This symptom is observed on ASR 1000 Router Series running Release 2.5.1 with GETVPN set up.

  Workaround: There is no workaround.

- CSCte97814

  On an ASR 1000 Router with BGP enabled, a small fixed size chunk memory leak is observed during boot-up. To be exact, it is observed just after config bulk-sync in redundant RP setup.

  This symptom is observed on Cisco ASR 1000 Series Routers with a redundant RP setup and BGP enabled.

  Workaround: There is no workaround.

- CSCtf01618

  A Cisco ASR 1000 router may unexpectedly reload due to SegV error.

  This symptom is observed on Cisco ASR 1000 routers running 12.2(33)XND1 or later XND or later 12.2(33)XN and running DMVPN with tunnel protection.

  Workaround: Move to unaffected release or remove tunnel protection.

- CSCtf06845

Cisco ASR 1000 Router crashes when receiving a crafted SNAP header.

This symptom is observed on ASR 1000 Router Series when a packet is receiving on a "encapsulation dot1Q" interface.

Workaround: There is no workaround.

- CSCtf12319

  ASRNAT with intrabox redundancy and PAT configuration in rare cases may retain session on the active much longer than what is configured (up to 4.5 hours).

  This symptom is observed when ASRNAT is running with intrabox redundancy and PAT configuration.

  Workaround: Set NAT timeouts to 15 seconds or less. Disable the second ESP.

- CSCtf12623

  A low memory condition can be seen on a Cisco ASR 1000 Router when NAT MIBs are queried.

  This symptom is observed on ASR 1000 Router Series when NAT MIBs are queried.

  Workaround: The workaround would be to exclude NAT MIB as following:

```
R5-mcp-4ru-2(config)#snmp-server view  test  1.3.6.1.4.1.9.10.77.1 excluded
R5-mcp-4ru-2(config)#snmp-server view test internet included
R5-mcp-4ru-2(config)#snmp-server community pub view test RO
```

- CSCtf15848

  The following error is seen on re-configuring channel-groups after switchover:

  EFC ERROR: spa_efc_config_ds1_channel - channel in use

  This symptom is observed with the following steps:

  1. The active RP is booted with 8xcht1/e1 and channel-group is configured on t1 controller
  2. Load the standby RP, and do a switchover
  3. On new active RP, unconfigure and reconfigure the channel-group

  Tracebacks with **EFC ERROR: spa_efc_config_ds1_channel -channel** in use are seen.

  Workaround: Before switchover, configure channel-groups on active RP when standby RP is up.

- CSCtf16359

  ASR 1000 Series Router configured as GETVPN GM will not make any local GM ACL change of removing extended ACL effective, until a new rekey from Key server.

  This symptom is observed on ASR 1000 Router Series configured as GETVPN GM.

  Workaround: There is no workaround.

- CSCtf19748

  FP crash seen on the BR with IOS XE 2.6 image. The crash happens when the MC is loaded with scaled configuration and http/ftp traffic is running.

  This symptom is observed under the following conditions:

  1. Load basic config on the MC (single prefix list, single active probe and single traffic application class).
  2. Send traffic matching the application traffic class.
  3. Load scaled configuration(ex 500 traffic classes)

  Workaround: There is no workaround.

- CSCtf22256

  FP reloads on ASR 1000 Router Series.

  This symptom is observed on ASR 1000 Router Series when using **show platform hardware qfp active feature wccp service id <*service id*>** after service is not configured.

  Workaround: Do not used show command **show platform hardware qfp active feature wccp service id <*service id*>** before valid WCCP configuration.

- CSCtf27981

  ASRNAT static network does not work properly or traceback may be received on configuration on unconfiguration.

  This symptom is only observed if 2 static networks are configured exactly the same except for network mask.

  For example:

```
ip nat inside source static network 10.1.0.0 10.2.0.0 /24 vrf vrfA
ip nat inside source static network 10.1.0.0 10.2.0.0 /16 vrf vrfA
```

  Workaround: Do not configure 2 static networks exactly the same except for network mask. If you do, it is recommended that you do the following:

  1. Remove both static network configuration
  2. Add back the 1 static network which is truly desirable.
  3. That should work, but if it does not reload the box.

- CSCtf30416

  When calling endpoint does not support T.38, the fallback is not working.

  Workaround: There is no workaround

- CSCtf32693

  On a Cisco ASR 1000 Router Series, configuring xconnect on a VLAN, SNMP 64 bit counters are not getting updated.

  This symptom is observed on a VLAN with xconnect configuration on same port.

  Workaround: There is no workaround.

- CSCtf33956

  Fragmented UDP or TCP DNS response processed by NAT ALG will be dropped.

  This symptom is observed when a DNS response is going through an ASR 1000 Series static NAT router running release 12.2(33)XND2.

  Workaround: There is no workaround.

- CSCtf40199

  A DNS response going through NAT ALG will not have the payload TTL changed 0 for same pre/post static config.

  This symptom is observed when a DNS response is going through an ASR 1000 Router Series static NAT router running release 12.2(33)XND2.

  Workaround: There is no workaround.

- CSCtf40592

  Higher latency for priority packets is observed.

For ethernet, when configuring model F broadband configuration using ANCP to change the shape rates on individual VLANs, higher latency for priority packets may be encountered. The same issue may be encountered if you remove the shaper policy-map from the VLAN and then re-apply it.

For ATM, when using multiple ATM VCs per physical interface, sustained oversubscription of that same physical interface may result in higher latency for some priority packets.

Workaround: Ethernet: Do not change the shape rate on a VLAN.

ATM: Avoid oversubscribing the interface for a sustained period of time."

- CSCtf40702

  A Cisco ASR 1000 Router Series with Route Processor 2 engine may unexpectedly reload due to a SegV crash.

  This symptom is observed if there is a monitor session configured that uses a source interface with a range. This can either be a crash while configuring via CLI or a crash at bootup if the command is in the startup config.

  Workaround: Do not use the source inter range.

- CSCtf43345

  Active and Standby FP resets on Cisco ASR 1000 Router.

  This symptom is observed during longevity run with LDAP, DNS traffic and continuous SNMP MIB Walk.

  Workaround: There is no workaround.

- CSCtf48067

  Memory leakages occur after configuring and de-configuring various netflow configurations. This includes any interface type on which netflow is configured: physical, VLANs, VT sessions, and so on.

  This symptom is observed after the following steps:

  1. Configure/De-configure netflow on physical interface.
  2. Configure/De-configure various caches.3.Configure/De-configure sub-interface(s) which has netflow enabled on it.
  3. Exporter configuration change on main and aggregation cache.
  4. Configure/De-configure virtual-interface(s) created using virtual template which has netflow enabled on it.
  5. Configure/De-configure various samplers.

  Above condition independently also leads to memory leakage.

  Workaround: There is no workaround.

- CSCtf51450

  During regular operations, the following log message was observed:

  ```
  IOSXE-6-PLATFORM: F0: cpp_cp: QFP:00 Thread:032 TS:00005645124008456668
  %LOGGER-6-DROPPED: 1 messages
  ```

  The intensity of this message was very high causing buffer and syslogs to be filled up with unwanted messages.

  This symptom is observed on ASR 1000 Router Series, running with 12.2(33)XND Release.

  Workaround: Consider filtering messages. Make use of ESM to drop these messages selectively from any of the targets (buffer, Vty/Console OR the syslog server).

- CSCtf61700

  Memory leak seen with the Radius process.

  This symptom is observed when a Radius Server (ACS) sends Access-Reject for a service profile download.

  Workaround: Make sure the service profile to be downloaded is configured in the ACS (Radius server).

- CSCtf65536

  ESP can crash while performing SIP calls using Cube-SP function.

  This symptom is observed when hairpinned SIP calls are present, but it is timing related, so it doesn't occur in all cases.

  Workaround: There is no workaround.

- CSCtf70851

  Input/Output Rate freezes and doesn't get updated.

  This symptom is observed if the interface is **shut** with the traffic running, the input/output rate gets stuck and doesn't go back to 0.

  Workaround: Giving **no shut** on the interface restarts the input/output rate.

- CSCtf85841

  The memory usage shown in the following commands keeps increasing as we repeatedly activate FRR and de-activate it by shutting and un-shutting relevant interfaces:

  sh platform software memory forwarding-manager f0 brief | inc CPP CEF MPLS MPLS

  sh platform software memory forwarding-manager f0 brief | inc frr

  This symptom is only observed if FMAN-RP receives the FRR delete request before receiving the delete request of all its child objects (out-of-order events).

  Workaround: There is no workaround.

- CSCtf86998

  In a GETVPN ASR 1000 Router Series deployment, packets on one of the ASR GM router interfaces are not encrypted.

  This symptom is observed when GM1 is in passive mode.

  Workaround: There is no workaround.

- CSCtf98758

  Standby RP crashes after replacing the basic configuration of the router with an au3-e3 configuration.

  This symptom is observed after intiating the following steps:

  1. Configure the router with back-to-back SDH link for full AU3-E3 configurations with SPA-1XCHOC12/DS0.
  2. Save the running configuration using **copy run bootflash:au3-e3.conf**
  3. Reload the router with config register set to 0x2142. This will get the router running configuration to the basic default configuration.
  4. After the router is up with redundancy setup and basic default configuration, execute the config replace command with the target config that was saved in step 1. {Config replace bootflash:au3-e3.con}

Workaround: There is no workaround.

- CSCtf98802

  Config replace command when executed in a particular way causes the router to malfunction.

  This symptom is observed after the following steps:

  1. When we try to remove channelized configuration using config replace command, it will ask for the confirmation of the same as below:

  Unprovision clear channel interface ?[confirm]

  2. If we put any character other than 'y' or 'n' it will not remove the channel configuration for that particular path.
  3. Now, if I try to remove these channels that were not cleared before manually, the system is behaves improperly:

```
Router(config-controller)#au-3 1
%ERROR: Standby doesn't support this command                            ^
% Invalid input detected at '^' marker.

Router(config-controller)#
As you see above system is not allowing to enter into the controller configuration
mode and resulting into "%ERROR: Standby doesn't support this command" message.
```

  Workaround: By this point of time only after reload of the router, the situation comes under control and then only we can alter the controller configurations.

- CSCtg00292

  Some translations getting stuck in standby router and with a **show ip nat trans verbose** we can see they have use_count as zero. This symptom is observed in a B2B NAT scenario and can happen while scaling.

  Workaround: Resetting the FP is the only workaround.

- SCtg06681

  SIP method profile allows defining a mapping of status-codes. RP2 CUBE(SP Edition) would crash while removing status-code map.

  This symptom is observed in the following configuration:

  For RP2 CUBE(SP Edition), consider the following config:

```
config t
sbc test
 sbe
  sip method-profile SIPmessage
    method INVITE
     action as-profile
     map-status-code
      range 183 value 180     <==== incorrect mapping
end
```

Note That there is only one entry for mapping status-code.

  When we try to unconfigure "range 183 value 180" as follows

  the RP2 CUBE(SP Edition) would crash:

```
config t
sbc test
 sbe
```

```
  sip method-profile SIPmessage
    method INVITE
     map-status-code
     no range 183 value 180  <=== causes crash
end
```

Workaround: The workaround is to unconfigure "map-status-code" and then re-configure it with correct mapping of status-code as follows:

```
config t
sbc test
 sbe
  sip method-profile SIPmessage
    method INVITE
    no map-status-code      <==== unconfigure map-status-code

    map-status-code         <==== re-configure
      range 180 value 183   <==== correct mapping
end
```

- CSCtg08753

  When using ASRNAT HA, if sessions on active are under SYN, RST or FIN timeout value and a switchover occurs, timeout value for those sessions goes back to TCP timeout on the new active instead of properly honoring SYN, RST, FIN timer.

  Workaround: There is no workaround.

- CSCtg23281

  At times with IP header compression enabled, the RTP timestamp is not restored to its correct value after compressing/decompressing the IP/UDP/RTP headers. This can cause jitter or one way audio. The issue occurs when an ASR 1000 Series Router is the compressor and a Cisco 2800 ISR is the decompressor.

  This symptom is observed when IP Header Compression is enabled in either Cisco original or IPHC format between an ASR 1000 Router Series and a Cisco 2800 ISR.

  Workaround: Use IETF IP Header Compression instead of Cisco original or IPHC format.

  ip rtp header-compression ietf-format periodic-refresh

- CSCtg30921

  ASRNAT pool shows allocated count of 1 when there are no addresses allocated. This means the pool can not be removed even though there are no translations off the pool.

  There is a very small timing window where this symptom occurs only for pool overload configuration. This window can happen when **clear ip nat trans *** is issued as translations are aging out. It is more likely to be seen if there are a very large number of overloaded pools.

  Workaround: The box or ESP must be reset to recover from this situation. "

- CSCtg45583

  MLP QFP client leaks memory.

  This symptom is observed if a QOS service-policy with many (7+) class-maps is configured on a Multilink interface.

  Workaround: There is no workaround.

- CSCtg52972

Configuring **ip flow-export template options sampler** on an ASR 1000 Router may stop Netflow from working and this may cause errors. It is not supported, so the command should be rejected at the CLI.

This symptom is observed when configuring the unsupported feature **ip flow-export template options sampler** on an ASR 1000 Router.

Workaround: Reload.

- CSCtg81294

  When trying to remove ASRNAT dynamic pool, the following message is observed even when there are no translations:

  %Pool <pool-name> in use, cannot destroy

  This symptom occurs in rare conditions of aging when the command **clear ip nat trans *** is run.

  Workaround: Unfortunately the only work around is to reload the box. This problem has been fixed and is only expected to be seen in B2B EFT image which just missed the fix.

Open Caveats—Cisco IOS XE Release 2.4.3

This section documents possible unexpected behavior by Cisco IOS XE Release 2.4.3.

- CSCsz01980

  The RP1 may experience unexpected watchdog timeout and reload.

  Under very rare conditions, an RP1 may experience a watchdog timeout during boot or shutdown and subsequently generate a kernel core dump.

  Workaround: No known workaround; following reload, the RP works as expected.

- CSCta24676

  On the ASR 1000 Router when an attempt is made to login to the kerberos client, the RP crashes. This is after the clocks of the UUTs are synchronized and the routers are configured with kerberos credentials.

  Workaround: There is no known workaround.

- CSCta27191

  On the ASR 1000 Router when used “upgrade rom-monitor filename harddisk:asr1000-rommon.XND.pkg all” for upgrading ROMMON the rommon failed to upgrade RP1 board on 6RU (RP2) chassis.

  Workaround: There is no known workaround.

- CSCta37670

  The ASR 1000 Router crash as a longer interrupt hold, when a single MPLS scales up to 300K prefixes. This issue occurs only when a single MPLS with 300K prefixes. The issue does not occur with 100 prefixes.

  Workaround: Not to run 300 prefixes

- CSCta76460

  On the ASR 1000 Router IPSEC EZVPN tunnels may get lost (not rekeyed properly) after a few rekey intervals.

  Workaround: Increase the rekey interval to maximum to avoid the frequency of rekeying.

- CSCtc38036

The file table overflow error will occur when the file system is being accessed.

This will occur after a few days on the ASR 1000 Router Series when running 2.4.1 and 2.4.2:

router#more system:running-config

%Error opening system:running-config (File table overflow)

Workaround: Reloading the router solves the problem, but it appears again after a few days.

- CSCtc75736

  When EIGRP is configured on the ASR 1000 Router Series the MVPN Hub role stops sending acknowledgements for reliable packets. This condition on occurs when GRE Multipoint Tunnel **shut/no shut** has been applied.

  Workaround: None

- CSCte19727

  Some IPv6 Bi-directional entries will not forward traffic on a Cisco ASR 1000 Router.

  This instance can occur when IPV6 PIM-SM and IPv6 PIM-Bi-directional are both configured on the router.

  Workaround: None

- CSCte50721

  During stateful NAT sync of H323 information from primary to standby, the standby crashes.

  This condition occurs when Cisco ASR 1000 Router with dual RP and ESP configured.

  Workaround: Is to disable H323 with the following commands when H323 ALG is not required:

  no ip nat service h225

  no ip nat service ras

- CSCte56627

  Outside NAT sessions are not syncing between active and standby.

  The following symptom may occur:

  1. Sessions may not be sync properly to standby OR
  2. session deletes may not be sync properly to standby (session that would be deleted on standby, will not be deleted).

  The following conditons may occur:

  1. On ASRNAT when there is an inside mapping and outside static mapping configuration.
  2. When there is a very high burst of session aging occurs.

  Workaround: None

- CSCte60069

  During the scale testing with ModelF applied on PTA, reparenting operation results in FP crash. Also CPUHOG and TIMEHOG tracebacks observed. The following conditions have been seen:

  1. On PTA, bring up 24K IPv4 sessions, 2PQ+2CQ (modelf)
  2. remove grandparent shaper and3)add the shaper back. When this instance occurs, FP crashes a tracebacks are observed.

  Workaround: Without the fix for this ddts, avoiding reparenting with large number of vlans with sessions will resolve the issue.

- CSCte77136

CLNS routing over GRE tunnels is not working on the ASR 1000 Router Series. When CLNS routing over GRE tunnels is configured, specifically with a GRE tunnel as the egress interface (output from the ASR 1000 Router). The CLNS packets are not forwarded via fast switching.

Workaround: Use the following configuration change on a per interface basis: **no clns route-cache** disables the clns fast switching.

- CSCte89787

  A Cisco ASR 1000 Router crashes after the Segment Switch manager reports that an invalid segment has been detected. The following logs appear on the console:

  %SW_MGR-3-INVALID_SEGMENT: Segment Switch Manager Error - Invalid segment - no segment class.

  The router will crash followed by this message.

  This has been observed on an ASR1002 running 12.2(33)XND1.

  Workaround: None known so far.

- CSCte91533

  A Cisco ASR 1000 Router is dropping small fragmented udp packet and udp fragments less than 28 bytes.

  This occurs when Windows XP Client login process to an Active Directory server in DC is slow. After the Windows client is connected to a branch site and running GETVPN across an MPLS cloud. The Cisco ASR 1000 Router is acting as a GETVPN GM Headend router.

  Workaround: None

- CSCte97907

  A Cisco ASR 1000 Router with RP2 gets out of sync with NTP master every 18 minutes for approximately 1 minute. The offset to the NTP master increases up to -1052.1 msec and the sync gets lost.

  This occurs when NTP is **enabled** and running aproximately 20 minutes.

  Workaround: None

- CSCtf01618

  A Cisco ASR 1000 Router may unexpectedly reload due to SegV error.

  This condition has been observed, when the ASR 1000 Router must be running 12.2(33)XND1 or later XND or 12.2(33)XNE or even later 12.2(33)XN releases and DMVPN is configured with Tunnel Protection.

  Workaround: Remove Tunnel Protection.

- CSCtf04257

  On a Cisco ASR 1000 running IOS XE 12.2(33)XND1 below message may be seen, when trying to configure a EoMPLSoGRE VC: %SW_MGR-3-CM_ERROR:

  Connection Manager Error - provision segment failed [SSS:Eth:<number>] - no resources available.

  This condition has been seen on Cisco ASR 1000 Router, running IOS XE 12.2(33)XND1. When destination of VC is changed from original to something else and then changed back to original.

  Workaround: None.

Resolved Caveats—Cisco IOS XE Release 2.4.3

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.4.3

- CSCse97209

  On a Cisco ASR 1000 Router Series standard communities are not set correctly by an outbound route-map.

  This occurs when ***route-map uses*** continue option is used.

  Workaround: There is no workaround.

- CSCsk85192

  On a Cisco ASR 1000 Router copy command arguments followed by a ":" are not sent to ACS when command authorization is enabled. This includes scp:, ftp:, tftp:, flash:, etc. On enabling parser ambiguity debugs its seen that the arguments with colon are not matched with the existing keywords though its a valid directory.

  Workaround: Is to deny or permit the full copy command for users.

  Further Problem Description: This issue affects AAA Authorization. When the argument is specifically denied by ACS that arguement will be able to be run on the IOS device. If the arguement is specifically allowed by ACS with default arguements being denied the commany followed by a ":" will not be able to be run.

- CSCso18626

  Destinations via MLPPP sessions may become unreachable following a RP switchover. When MLPPP sessions are active, BGP nexthops are reachable via the MLPPP session prior to a switchover. An RP switchover then occurs.

  Workaround: The affected multilink interfaces can be shut/no shut i.e.

  shut/no shut interface multilink

  Repopulating the routes in the affected VRF(s)will also restore reachability.

  clear ip route vrf FOO

- CSCso18626

  Destinations via MLPPP sessions may become unreachable following a RP switchover. When MLPPP sessions are active, BGP nexthops are reachable via the MLPPP session prior to a switchover. An RP switchover then occurs.

  Workaround: The affected multilink interfaces can be shut/no shut i.e.

  shut/no shut interface multilink

  Repopulating the routes in the affected VRF(s)will also restore reachability.

  clear ip route vrf FOO

- CSCso60442

  A crash occurs on a Cisco ASR 1000 Router Series.

  This symptom is observed when the **show buffers interface dump**command is entered.

  Workaround: There is no workaround.

- CSCsv36976

  After the display of the 1000 characters on the console, if there are more to display, the display is truncated. The problem happens when you have large number of interfaces and the output of "show zone security" is larger than 1000 characters.

Workaround: The workaround is to show all interfaces and get the zone membership from the interface.

Further Problem Description: The root cause of the problem is that the display buffer for this command is limited with 1000 characters."

- CSCsv36976

  A Cisco ASR 1000 Router running IPSec (IP Security) can run at high cpu up to 100% indefinitely in the “Crypto IKMP” process.

  This problem can occur when there is error conditions internal to the IKE process.

  Workaround: The workaround is to issue the command **clear crypto isakmp** to clear theIKE SA's.

- CSCsx10028

  A core dump may fail to write or write very slowly (less than 10KB per second) on the Cisco ASR 1000 Router Series.

  The symptom is observed when the cause of the crash is processor memory corruption. When this occurs, the corrupted memory pool cannot be used to write the core dump so it will likely fail. (IO memory corruption crashes should not have this problem.)

  Workaround: There is no workaround.

  Further Problem Description: This bug also increases the default size for the exception memory region to 256K to make sure it has enough memory to handle writing core dumps. This means that it is no longer necessary to adjust it as per the core dump instructions on CCO.

- CSCsx15841

  The **BGP aggregate-address** command configured on active RP does not auto-sync to the running configuration of the standby RP.

  This occurs when BGP is configured on active and standby redundant RP system(s).

  Workaround: Configure BGP aggregate-address and reboot the system, forcing both active and standby to load from startup configuration.

- CSCsx30395

  When all interfaces are **shut**, wait 5 secs, and then **no shut**, then LDP session is not reestablished for one link peer. This seen only on ASR 1006 with VPNs on GigE dot1q interfaces, some with AToMPLS.

  Workaround: Clear sessions with **clear mpls ldp nei ***.

- CSCsx83443

  ISKMP debug messages from all peers are shown in the terminal monitor enable tty/vty's even though **debug crypto condition peer ipv4 x.x.x.x** is set.

  This condition can occur when using peer IP-based debug condition.

  Workaround: There is no workaround.

  Further Problem Description: Only a subset of the messages are shown.

- CSCsy10893

  A Cisco ASR 1000 Router reloads occasionally after the command **show buffers leak** is repeatedly issued.

  The symptom is observed when issuing the **show buffers leak** command. This occurs only with certain patterns and scale of traffic and does not occur all the time.

Workaround: There is no workaround.

- CSCsy45371

  The **clear ip nat tr *** command removes corresponding static NAT entries from the running configuration, but removing static NAT running configuration does not remove the corresponding NAT cache.

  This may occur, when NAT commands are entered while router is processing around 1 Mb/s NAT traffic.

  Workaround: Is to stop the network traffic while configuring NAT.

- CSCsy49927

  The IOSd restart is seen with crest proc frame that fetches the tcl shell for execution.

  This is seen with crest proc that helps in configuring a scale configuration.

  Workaround: None

- CSCsz15295

  The GM failed to register when fail-close feature is enabled with missing ACL.

  This instance has occurred when configuring fail-close that gives a matching ACL and activates. In addition, do not configure ACL in global configuration.

  Workaround: Is to deactivate fail-close.

  Further Problem Description: GM failed to register when fail-close feature is configured with a non-existing ACL.

- CSCsz56462

  When configuring cdp run it does not bring up cdp on the interfaces. This Conditions happens only if the default behaviour of a platform is to have CDP disabled.

  Workaround: To enable CDP, include the cdp enable command in the configuration.

- CSCsz72591

  On a Cisco ASR 1000 Router crashes with an Address Error (load or instruction fetch) exception. The router must be configured to act as a DHCP client.

  Workaround: There is no workaround.

- CSCsz74859

  NHRP cache entry is not getting created for certain spoke nodes on a Cisco ASR 1000 Router Series.

  This symptom occurs when two spokes A and B advertise the same subnet with varying masks (anything other than /8 or /16 or /24). A third spoke upon receiving such routes (from the hub), in order to send traffic to such subnets, can form a dynamic tunnel with either A or B but not both at the same time.

  Workaround: There is no workaround.

  Further problem description: There is no hindrance to traffic since it continues to flow via the hub. When tunnel with spoke A is formed, there is no problem with traffic to subnet behind spoke A. But, traffic to subnet behind spoke B takes the spoke A - hub - spokeB path. This can be easily noted by traceroute.

- CSCta26029

  Path attribute memory leak is found when there is some path attribute churn in the network.

  The symptom is seen only when there are idle peers on the router.

Workaround: Unconfigure the idle peers.

- 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.

- CSCta48816

  On a Cisco ASR 1000 Router running ODR as a routing protocol for a DMVPN deployment, might display similar message:

  Jun 9 03:40:44.141: %SYS-2-GETBUF: Bad getbuffer, bytes= 32717 -Process= "CDP Protocol", ipl= 2, pid= 157

  These messages have been seen on Cisco ASR 1000 Router running software 12.2(33)XNC1.

  Workaround: Use a routing protocol which does not rely on CDP in the DMVPN cloud (passive RIP, RIP, BGP or EIGRP).

- CSCta93640

  Next-hop tracking notification is sent even though track is undefined. This has been observed, when PBR is configured with the set next-hop tracking.

  Workaround: None

- CSCtb13421

  The GM may not register on a Cisco ASR 1000 Router Series. This symptom has been observed, when a crypto map with local-address is configured and applied on multiple interfaces, after one of these interfaces are then shut.

  Workaround: Is to disable local-address for the crypto map.

- CSCtb32502

  With a 1K DMVPN spoke, unconfigure/ re-configure tunnel protection several times and unconfigure/re-configure a tunnel interface, the RP resets.

  Workaround: Wait until all DMVPN session is up or down before next unconfig/re-config tunnel. That is, do not unconfig/re-configure tunnel when there are many sessions in transaction state.

- CSCtb67461

  When pado delay per circuit id is configured for different strings in the PTA device, the circuit id needs to be matched with each entry in the list until a match is found. But this does not happen. Only the first string is tried to be matched and if a match not found, no pado delay is applied. This is the same case for remote id.

  Workaround: None

- CSCtb74547

  On a Cisco ASR 1000 Router Series DMVPN HUB reloads when processing IPSEC key engine.

  This conditions happens when dual DMVPN with shared tunnel protection feature is enabled.

  Workaround: None

- CSCtb89424

In rare instances, a Cisco ASR 1000 Router may crash while using IP SLA UDP Probes configured using SNMP and display an error message similar to the following:

hh:mm:ss Date: Address Error (load or instruction fetch) exception, CPU

signal 10, PC = 0x424ECCE4

This symptom is observed while using IP SLA on the router.

Workaround: There is no workaround.

- CSCtb89767

  A problem may occur on an FP20 when configuring the IPSEC part of the SVTI topology the delete and reconfig of IPsec does not happen. This has been seen in a FP20 SVTI IPSEC setup with 1 tunnel configured.

  Workaround: Is to reload the router.

- CSCtc21042

  A chassis-manager processed on RP2 gets stuck and the router becomes unresponsive to user commands. All the FPs and CCs keep rebooting, with console logs showing repeated FP code downloads.

  This problem is specific to RP2. No particular scenario is known. Problem is caused by OBFL logging of messages on RP2.

  Workaround: Is to disable onboard logging of messages on RPs as follows:

  “hw-module slot r0/r1 logging onbaord disable”

  Router#hw-module slot r0 logging onboard disable

  To verify that onboard logging has been disabled:

  Router#sh logging onboard slot r0 status

  Status: Disabled

Note This command is not saved in the config so is not preserved across router reloads.

- CSCtc25464

  After the ASR 1000 Router Series has been reloaded, and the tunnel interface has been configured with keepalives it will remain in the line-protocol down state. This will occur only when keepalives are configured for a short interval (total timeout under 10 seconds) and when the box has been reloaded.

  Workaround: Is to remove the keepalive configuration on the tunnel and to reload the configuration again; after the router has rebooted when the tunnel interface is still down.

- CSCtc30420

  CPP tracebacks are logged after configuring the ASR 1000 Router Series as an RP2 with IPSec DMVPN Spoke. Only in this condition, when unconfiguring DMVPN on the router and reconfiguring it again, CPP tracebacks are logged.

  Workaround: Is to reload the router.

- CSCtc38484

  The giga word counters are not reflecting properly in the stop record.

  When the interim accounting is enabled, the giga-word counters are reflecting fine in interim and stop record. This occurs on the ASR 1000 Router.

Workaround: There is no issues when the interim record is enabled. When the interim accounting is disabled on the ASR 1000 Router, execute the show interface virtual command. This will allow for the giga word counter in the stop record to be confiigured.

- CSCtc40677

  The distribute-list applied to the virtual-template interface is not effective for the virtual-access interfaces spawned by that template.

  For example, configured on the ASR (hub) is:

```
router eigrp 1
 redistribute static metric 10000 100 255 1 1500
 network 10.0.0.0
 no auto-summary
 distribute-list prefix TEST out Virtual-Template1!
ip route 0.0.0.0 0.0.0.0 Null0
ip route 10.0.0.0 255.0.0.0 Null0!
ip prefix-list TEST seq 10 permit 0.0.0.0/0
ip prefix-list TEST seq 20 permit 10.0.0.0/8
```

  For example: On the branch site when connected to a Virtual-accessinterface will show as:

```
ranch#sh ip route eigrp
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, *15:56:44.397 BRU Wed Oct 7 2009
10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D       10.0.0.0/8 [90/46251776] via 10.12.0.2, 00:00:06, Dialer1
D       10.1.1.0/24 [90/46228736] via 10.12.0.2, 00:00:06,Dialer1
D       10.2.2.0/24 [90/46354176] via 10.12.0.2, 00:00:06, Dialer1
D*EX 0.0.0.0/0 [170/46251776] via 10.12.0.2, 00:00:06, Dialer1
```

  This shows that no filtering was applied, since the 10.1.1.0/24 and 10.2.2.0/24 should have been dropped off the updates.

  The symptom is observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 12.2(33)XND1.

  Workaround: Configure the distribute-list for the specific virtual-access interface used for the connections on the hub.

- CSCtc43110

  Under H.323 call scenarios, outgoing H.323 signaling packets (TCP) are marked with a non-zero DSCP value, even though no QoS is configured for H.323 calls. This happens under all H.323->H.323 and SIP->H.323 scenarios when SBC creates a downstream H.323 calls.

  Workaround: There is no workaround with SBC configuration. QoS can be re-marked when MQC policy is placed on the outbound physical interfaces of the ASR 1000 Series Router.

  Workaround: None

- CSCtc45681

  QoS Accounting stats is incorrect after changing the policer rate.

  The following conditions have been observed:

  1. ASR1004 is configured as PTA.
  2. QoS Accounting is enabled at the output policy-map voip class.
  3. Pass traffic for 10 seconds.
  4. Stop traffic and verify the interim-update record has the correct QoS accounting stats.
  5. Re-start traffic.

6. Under traffic load, modify the voip class police rate.
7. Verify the voip traffic is now policed to the new rate.
8. Stop traffic.
9. Run show cmd: show policy-map session output.

Note Note the voip class conformed pkt/byte counts.

10. Check the accounting interim record. Notice that the pkt/byte counts do not match those form the show cmd output in step 9.

Workaround: Remove and reapply the QoS policy-map.

- CSCtc51048

  On the Cisco ASR 1000 Router the FP will reset, when configuring "**show platform hardware cpp feature ipsec spd all**" on the cli, after deleting tunnels FP crash on "**sh pla hard cpp feature ipsec spd all"** while deleting tunnels. This condition will occur when tunnel has been deleted and applyed to the CLI "**show platform hardware cpp feature ipsec spd all**" both even should happen together.

  Workaround: Do not apply CLI "**show platform hardware cpp feature ipsec spd all**" while you are deleting number of tunnels.

- CSCtc53381

  Encryption with decryption fails after deleting and creating a IPSecv6 Tunnel on a Cisco ASR 1000 Router.

  This problem is seen after deleting and recreating a IPSecv6 Tunnel.

  Workaround: None

- CSCtc65800

  FP reloads when crypto map is removed from interface in CAC-ACL configuration on a Cisco ASR 1000 Router.

  This occurs only when CAC ACL configuration is used. Plain ACL with match address will not have any FP reload issue.

  Workaround: None

- CSCtc65800

  A virtual reassembly error message of the FRAG-REASSEMBLY_DBG type is seen and the traceback decode of the error message points to the ipv4 vfr refrag function indicating packet drop. The issue may cause another ATTN_NOTIFY timeout error message in about 4 minutes.

  The condition was observed under uRPF drop on broadband LNS virtual interface. In general other virtual reassembly drops at ipv4 vfr refrag due to malform fragments may trigger the issue.

  Workaround: Un-configure vitrual reassembly or avoid the specific packet drop condition.

- CSCtc68037

  A Cisco IOS XE device may experience an unexpected reload as a result of mtrace packet processing.

  Workaround: None other than avoiding the use of mtrace functionality.

- CSCtc86951

On the ASR 1000 Router Series, when high speed logging is enabled for NAT, ESP may fail after a RP SSO switchover. In rare conditions when high speed logging is enabled for NAT, ESP may fail after a RP SSO switchover.

Workaround: None

- CSCtc87822

  On a PE router, eBGP-learned VRF routes might not be advertised to eBGP neighbors in the same VRF.

  The symptom is observed if DUT first learns the route from IBGP-VPNv4 (same RD) and then learns the route from the CE.

  Workaround: Soft clear towards the CEs missing the routes.

- CSCtc95423

  Router crashes when quickly unconfiguring and reconfiguring crypto maps on a Cisco ASR 1000 Router.

  This may only occur, when crypto is turned on while SAs are still being deleted in the background and duplicate SAs may be created, which may cause the router to crash.

  Workaround: Before re-applying crypto maps, wait until all SAs on the router are deleted before turning crypto back on.

- CSCtc96161

  DMVPN is working fine for a ~week and then one of spokes appears to be no longer able to pass traffic to other spokes. IPSEC tunnel between the spokes can be established at IOS level, but cannot be programmed into hardware and traffic is not getting through.

  This problem is only seen when there are more spoke to spoke dynamic tunnels and the dynamic tunnels are flapping frequently for a long period of time.

  Workaround: Reduce the frequency of dynamic tunnel flapping by increasing NHRP hold down timer to avoid tearing down dynamic tunnels too often. This can reduce the chance of hitting the problem. But when the problem happens, the affected spoke has to be reloaded.

- CSCtd00493

  For IPv6 Bi-directional entry FF03::1:0:0/96, some packet with address like FF03::1:1:1/128 or FF03::1:1:2/128, etc… In addition a Cisco ASR 1000 Router cannot find a match in CPP due to the collision lookup failure. This problem may cause the traffic to not forward the entries on the router.

  Workaround: None

- CSCtd00644

  The ASR 1000 Router Series may restart ungraceful with scaled config. When there is scaled config and sessions are flapping frequently, only on rare instances the ASR 1000 Router Series may restart ungracefully. This problem may also timing related, so it may not happen with every time sessions flaps.

  Workaround: None

- CSCtd02123

  WRED state only shows WRED state with standard class.

  In **sh policy-map int**, WRED state only show standard class's WRED state.

  Workaround: Is to only use standard wred classes.

- CSCtd02554

  The following error message may show up when AAA is used by the PPPoE:

%AAA-6-BADHDL: invalid hdl AAA ID 0, hdl CE010AA1, retired -Process= “SG CMD HANDLER”, ipl= 0, pid= 151

This could happen during the scalability test with large number of PPPoE sessions.

Workaround: None

- CSCtd15634

  Traceback seen on a Cisco ASR 1000 Router console indicating an error.

  This condition occurs when bringing up an L2-Connected ISG session and then immediately sending a non-stop Service Activation and Deactivation CoA.

  Workaround: Do not send a non-stop Service Activation and Deactivation CoA immediately after bringing up an L2-Connected ISG session.

- CSCtd17681

  Multicast hello packets are not encrypted by IPSec resulting in failure to setup OSPF with EIGRP sessions.

  This Issue has been seen in a DMVPN setup, or when a point to point Frame-Relay IPSec session is configured.

  Workaround: None

- CSCtd35091

  The input queue on ISG's access interface gets filled up causing the interface to wedge.

  The symptom is observed when an L2-connected IP session for a client exists on the ISG and traffic from that client comes in with a different IP address to the one used to identify the session. This traffic is dropped and interface wedging is observed.

  Workaround: There is no workaround other than a router reload.

- CSCtd38225

  When ISG is enabled and DHCP sessions re-start just around the time their leases expire, some sessions may get stuck dangling indefinitely. Sending DHCP DISCOVER message (i.e.: re-starting the CPE) will not restore the session. The affected subscriber(s) will not be able to establish a session.

  The issue seems to be a corner-case situation. It is observed when ISG is enabled and DHCP sessions re-start just around the time their leases expire.

  Workaround: The only known workaround is to manually clear the dangling session(s) using the **clear ip subscriber dangling <*time*>** command although this may not be a suitable workaround in a live production network.

- CSCtd39778

  The Cisco ASR 1000 Router may reset due to IOS failure, when ZBFW is configured with more than 16 match protocols and there are large an additional no match protocl statements in ZBFW class-maps.

  This has been seen, when an addition of more than 16 match protocol statements in a class-map is used for inspect policymap on the ASR 1000 Router.

  Workaround: Is to split the class-map with more than 16 match protocol into multiple class-maps, each with 16 or less match statements.

- CSCtd47550

  On an ASR 1000 Router configured with redundant RP's and a scaled ISG configuration, the ESP fowarding processor may reload during an RP switchover.

Defect requires redundant RPs and a scaled ISG configuration with many active ISG sessions. An RP switchover also seems to be a necessary condition.

Workaround: No known workaround.

- CSCtd47813

  Traffic loss may be seen after rekey between the Cisco ASR 1000 Router Series acting as GMs when modifying KS ACL. This may only occur, when a more specific permit statement has been added. In addition, when permit ip any any has been applied this will result in traffic loss when rekeying the router.

  Workaround: Is to keep permit ip any as the last acl in the KS ACL set.

- CSCtd48203

  On a Cisco ASR 1000 Router, after the last cache engine in a WCCP service group goes away, packets start getting dropped instead of being forwarded to original destination.

  This problem occurs when the last cache engine present in a WCCP service group becomes unavailable.

  Workaround: To overcome this problem, remove the global service group definition of the service group whose all CEs have become unavailable by using the following CLI conf t:

```
conf t
 no ip wccp <web-cache | service-group-id>
   (or)
Remove the redirect in config from the interfaces on which the service group is
attached, like
conf t
 int <interface name>
 no ip wccp <web-cache | service-group-id> redirect in
```

- CSCtd48500

  SNMP 64 bit counters not showing traffic. This has seen seen on ASR1002 running 12.2(33)XND1 and XND2 after deploying an AToM Circuit under it.

  Workaround: None

- CSCtd49249

  The following error message shows up during the uSBC config:

```
%Log packet overrun, PC 0x111B639, format:
%s

log:

config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#sbc test
Router(config-sbc)#sbe
Router(config-sbc-sbe)#adjacency sip sippa
Router(config-sbc-sbe-adj-sip)#no attach
Router(config-sbc-sbe-adj-sip)#account sipp-a
Router(config-sbc-sbe-adj-sip)#fast-register disable
Router(config-sbc-sbe-adj-sip)#remote-address ipv4 1.2.37.19 255.255.255.255
Router(config-sbc-sbe-adj-sip)#registration rewrite-register
Router(config-sbc-sbe-adj-sip)#signaling-address ipv4 107.1.1.1
Router(config-sbc-sbe-adj-sip)#signaling-peer 1.2.37.19
Router(config-sbc-sbe-adj-sip)#signaling-peer-port 5060
Router(config-sbc-sbe-adj-sip)#signaling-port 5088
Router(config-sbc-sbe-adj-sip)#attach

%Log packet overrun, PC 0x111B639, format:
```

```
%s
Router(config-sbc-sbe-adj-sip)#end
Router#
```

Workaround: None

CSCtd50125

GetVPN on a Cisco ASR 1000 Router GM fails to download the TEK information in the hardware [debug crypto ipsec output below] *Nov 27 02:20:38.323: IPSEC(download associate flow):

```
flow_info: in_flow_id: 2400005F, out_flow_id 24000060
    out_flow_enable: 0
    acl_line_num 1
    sadb_root_local_add: 172.16.0.1
local_proxy: , remote_proxy:
    in_spi: 35EB57B0, out_sp
*Nov 27 02:20:43.341: IPSEC(crypto_ipsec_create_transform_sas): Failed to attach
flowid to hw
*Nov 27 02:20:43.342: IPSEC(delete_sa): deleting SA,
  (sa) sa_dest= 172.16.0.1, sa_proto= 50,
    sa_spi= 0xD2A8F435(3534287925),
    sa_trans= esp-aes 256 esp-sha-hmac , sa_conn_id= 2093    sa_lifetime(k/sec)=
(0/115),
  (identity) local= 172.16.0.1, remote= 0.0.0.0,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4)
*Nov 27 02:20:43.342: IPSEC(update_current_outbound_sa): updated peer 0.0.0.0 current
outbound sa to SPI 3751CFC3
*Nov 27 02:20:43.342: IPSEC(delete_sa): deleting SA,
```

This condition has been observer, when IPv6 configured on the crypto map local address,

Workaround: Is to disable IPv6 and reload the box.

- CSCtd53112

  IOS reload occurs when on a Cisco ASR 1000 Router when ‘debug cond ip nat inside source static..’ command entered and NAT has never been configured on the box.

  Workaround: Enter 'debug cond ip nat' commands only after NAT has been configured.

- CSCtd54632

  System console may not response on the Cisco ASR 1000 Router Series.

  This symptom is observed on a Cisco ASR 1000 Router Series when functions as an IP Security (IPSec) termination and aggregration router, and when a self-signed cerificate is configured during Forwarding Processor (FP) is out of service.

  Workaround: There is no workaround. The console will be back to service when FP is active or when the request gets timeout'ed (around 480 seconds).

- CSCtd67034

  The following error message is seen on a Cisco ASR 1000 Router “%CPPHA-3-FAULT: F0: cpp_ha: CPP:0 desc:...” and accompanying crash dump of the CPP QFP complex.

  The various errors which have been seen in association with this problem include:

  “%CPPHA-3-FAULT: F0: cpp_ha: CPP:0 desc:...”

  where desc: could be any of the following errors:

  ```
  Desc: ETC_ETC_LOGIC1_LEAF_INT_INT_ETC_LKUP_DATA_ERR
  Desc: ETC_ETC_LOGIC2_LEAF_INT_INT_GPM_ENQ_VTL_DROP_ERR
  Desc: GAL_GAL_CSR_IPM_IF_GAL_IPM_IF_LEAF_INT_INT_IPM_ERR
  Desc: GRW_GPM_GRW_CSR_RDWR_UNIT_0_GPM_RW_LEAF_INT_INT_REQUEST_ERROR
  Desc: GRW_GPM_GRW_CSR_RDWR_UNIT_1_GPM_RW_LEAF_INT_INT_REQUEST_ERROR
  ```

```
Desc: GRW_GPM_GRW_CSR_RDWR_UNIT_2_GPM_RW_LEAF_INT_INT_REQUEST_ERROR
Desc: GRW_GPM_GRW_CSR_REQ_TOP_GPM_REQ_LEAF_INT_INT_MAP_ICREQ0_NO_CONTEXT
Desc: OPM_OPM_INT_REGS_OPM_META_LEAF_INT_INT_UNDEF_DESC
Desc: PQS_PQS_LOGIC1_INTR_LEAF_INT_INT_OUT_OF_RANGE_Q_ERR
Desc: SRT_SRT_PAR_ERR_LEAF_INT_INT_STEM_0
```

A corner case issue was discovered where the FRF.12 (Frame Relay Fragmentation) and MLP (Multilink PPP) features were susceptible to various hardware detected error conditions when performing fragment reassembly for cases where the last fragment was a few bytes in length (approx. 4-8 bytes of payload after the protocol headers).

This condition has only been seen with high traffic rates in conjunction with the small end fragment condition.

Workaround: None

- CSCtd70582

  Traffic Class services will remain in “show subscriber session” output under "Policy Information" after traffic class has disconnected by timer events.

  Only seen when Traffic Class is disconnected through an Idle Timer or Absolute Timer expiring.

  Workaround: When traffic class service is disconnected through normal (User Intervention), issue is not seen. For Timer disconnected Traffic Class services, no known workaround at this time.

- CSCtd79978

  A Cisco ASR 1000 Router crashes after issuing a “**show pppoe throttled subinterfaces** “command.

  This issue has been seen on ASR 1000 Routerrunning 12.2(33)XND2 IOS.

  Workaround: Not execute the show command.

- CSCtd90265

  IP Security (IPSec) functionality stops working, when Route Processor (RP) CPU rate can be high.

  This symptom is observed on a Cisco ASR 1000 Router Series when functions as an IP Security (IPSec) termination and aggregration router, after super package In-Service Software Upgrade (ISSU) was performed with IPSec traffic running.

  Workaround: There is no workaround.

- CSCte05638

  Cannot copy WebEx application logs from WebEx Node SPA console with Vegas shell commands.

  When connection to WebEx Data Center fails, the WebEx support team might need to look at the

  WebEx application log files to identify the problem.

  There is no mechanism today for customer to copy this logs files out of the WebEx Node SPA.

  Workaround: None

- CSCte19782

  When ESP traffic is traversing NAT with inside static configs, the traffic initiated from the outside hosts willl not work.

  This condition happens with NAT inside static configuration, the ESP traffic iniitated from the outside network will be passing through the NAT box untranslated.

  Workaround: There is no known workaround.

- CSCte20171

HSRP active router send ICMP redirect message that source address set to physical interface IP address. The Virtual IP address should be used as source address.

Workaround: None

- CSCte20928

  ESP20 restarts when loading the config on the RP2.

  This issue has been seen when loading config on a blank box with ESP20 and RP2.

  Workaround: None

- CSCte40621

  On a Cisco ASR 1000 Router when adding pinhole, after modify has failed with an ER=421 error message.

  For example: “AddIssue-NG.pcap” contains failed pattern with following order:

```
- ADD (pinhole ntt/user1a)
- ADD (pinhole ntt/user2a)
- Modify (pinhole ntt/user1a)
- ADD (pinhole ntt/user2v)   -> failed with ER=421
```

  Workaround: None

- CSCte45106

  Crash in QoS cpp_cp process when memory is running to slow on the Cisco ASR 1000 Router Series.

  The following conditions have been observed:

  1. Establish 25k PPPoE PTA ISG sessions with traffic classes, port bundle, l4r, accounting and QoS.
  2. Send traffic through the sessions.
  3. Make sure that all the idbs are used.
  4. Keep trying to establish PPPoE sessions.
  5. FP crash should be observed.

  Workaround: Keep memory from running low.

- CSCte45509

  The ASR 1000 Router cannot take over PPP and L2TP sessions when ISSU has been loaded .

  During ISSU step, active RP image is a previous version and Standby RP image

  is 12.2(33)XND3.

  The following traceback occur and cannot create ppp sessions on standby RP.

  %SYS-2-LINKED: Bad enqueue of xxx in queue xxx -Process= “RADIUS”

  Therefore all PPP sessions is lost at the time of RP switchover.

  Workaround: There is no workaround.

- CSCte46218

  Traffic is not forwarded through GRE or multipoint GRE tunnels with “tunnel key 0”. This condition is seen when tunnel key is configured via ""no tunnel key"" and then reconfigured via “tunnel key 0” on a GRE or mGRE tunnel, traffic will received tunnel packets will be dropped.

  Workaround: After removing tunnel key configuration, configure “tunnel key” with non-zero value or delete and recreate tunnel interface.

- CSCte89787

  An ASR 1000 Router crashes after the Segment Switch manager reports that an invalid segment has been detected.

  The following logs have been observed:

  %SW_MGR-3-INVALID_SEGMENT: Segment Switch Manager Error - Invalid segment - no segment class.

  The router will crash followed by this message.

  This has been observed on an ASR1002 running 12.2(33)XND1.

  Workaround: None

- CSCte91533

  A Cisco ASR 1000 Router may drop small fragmented udp packets, the udp fragments are less than 28 bytes. This condition has been observed when Windows XP Client login processes to an Active Directory server in the DC is slow. In additon, when Windows client is connected to a branch site and running GETVPN across an MPLS cloud. An ASR 1000 Router is acting as a GETVPN GM Headend router.

  Workaround: None

- CSCte97907

  On a Cisco ASR 1000 Router with RP2 gets out of sync with ntp master every 18 minuted for approximately 1 minute. This offsets the master and increases up to -1052.1 msec and the sync gets lost.

  This conditions may happen when NTP is enabled and running aproximately 20 minutes.

  Workaround: None.

- CSCtf14254

  Ucode crash has been seen with Multicast Nat configured on a Cisco ASR 1000 Router. This has been observed after configuring Multicast Nat on the router. This may cause a ucode crash.

  Workaround: None

- CSCtf18200

  Traffic loss during sub package ISSU for Release 2.4.3 to Release 2.6.0 after CC upgrade stage. This conditions has been seen when Gig based SPA interface with vlan is configured.

  Workaround: Traffic will resume once the RP upgrade is complete.

Open Caveats—Cisco IOS XE Release 2.4.2

This section documents possible unexpected behavior by Cisco IOS XE Release 2.4.2.

- CSCsy49927

  The IOSd restart is seen with RP2 at proc frame when using the tcl shell for execution. This is seen with crest proc that helps in configuring a scale config.

  Workaround: None

- CSCsz01980

  Under very rare conditions, the RP1 on a Cisco ASR 1000 Series Router may experience an unexpected watchdog timeout during boot or shutdown and reload.

  Workaround: None

  Following the reload, the RP1 works as expected

- CSCsz56462

  When configuring **cdp run** it does not bring up cdp on the interfaces. This Conditions happens only if the default behaviour of a platform is to have **CDP disabled**.

  Workaround: To **enable CDP**, include the cdp enable command in the configuration.

- CSCta22480

  When the **show memory debug leaks** or **show memory debug leaks chunks** command issues an output report it may not be accurate. In addition the **show memory debug leaks command** is not used under normal router operations; and this will not affect normal router behavior.

  Workaround: There is no known workaround.

- CSCta24676

  On the ASR 1000 Router when an attempt is made to login to the kerberos client, the RP crashes. This is after the clocks of the UUTs are synchronized and the routers are configured with kerberos credentials.

  Workaround: There is no known workaround.

- CSCta27191

  On the ASR 1000 Router when used "upgrade rom-monitor filename harddisk:asr1000-rommon.XND.pkg all" for upgrading ROMMON the rommon failed to upgrade RP1 board on 6RU (RP2) chassis.

  Workaround: There is no known workaround.

- CSCta37670

  The ASR 1000 Router crash as a longer interrupt hold, when a single MPLS scales up to 300K prefixes. This issue occurs only when a single MPLS with 300K prefixes. The issue does not occur with 100 prefixes.

  Workaround: Not to run 300 prefixes

- CSCta45697

  On the ASR 1000 Router high priority IPsec traffic could be dropped.

  This will occur When total throughput of high priority and low priority IPsec traffic oversubscribed the encryption/decryption engine.

  Workaround: Reduce IPsec traffic bandwidth to below threshold.

- CSCta48816

  On the ASR 1000 Router running ODR as a routing protocol for a DMVPN deployment, might display similar message:

  Jun 9 03:40:44.141: %SYS-2-GETBUF: Bad getbuffer, bytes= 32717 -Process= "CDP Protocol", ipl= 2, pid= 157

  These messages have been seen on ASR 1000 Router running software 12.2(33)XNC1.

  Workaround: Use a routing protocol which does not rely on CDP in the DMVPN cloud (passive RIP, RIP, BGP or EIGRP).

- CSCta76460

  On the ASR 1000 Router IPSEC EZVPN tunnels may get lost (not rekeyed properly) after a few rekey intervals.

  Workaround: Increase the rekey interval to maximum to avoid the frequency of rekeying.

- CSCtb07473

  On the ASR 1000 Series this is seen during router booted up after ISSU software upgrade and redundancy forceswitchover. This issue will occur when bringing up the console dump: show ipc session rx verbose, IOSd crashed at ipc_print_flow_control_statistics.

  Workaround: Use a local data structure to keep the contents of port_info.

- CSCtb07984

  he ASR 1000 Router acting as a LNS router failed to apply D2 QOS on first 2 PPPoX sessions after every new reboot and configures D2 QOS on all subsequent sessions. This occurs when PPPOX sessions are brought on LNS with D2 QOS model after new reboot of router.

  Workaround: LNS router configures D2 QOS on all subsequent sessions

- CSCtb29156

  The LNS will bring up Sessions without VRF configuration when Radius Customer template is used. The symptoms are when the PPPoX session are up and it will get the ip address from designated VRF pool.

  Workaround: Use local Customer template and vpdn configuration

- CSCtb49373

  On the ASR 1000 Router Series if there is no less than a specific static route including the prefix of the static route in the table it will stay in the routing table although both routes should be removed.The Static route pointing to next-hop (without exit interface) does NOT get removed from routing table when route towards next-hop disappears.

  Workaround: Specify an exit interface in addition of next-hop

- CSCtb51418

  On the ASR 1000 Router Series the RP will reload while flapping the sessions overnight.

  The RP will reload while running the following overnights:

  - Flap 8000 sessions once in every 20mins
  - ESIC,ISIC tools for sending invalid packets
  - RCMD script which does a rsh to the router and executes show commands continuously
  - Uploading files continuously to the router using tftp copy

  Workaround: None

- CSCtb56852

  RP resets when we delete DMVPN Tunnel on hub router .

  In 1hub and 1000 spokes scenario, when we delete dmvpn tunnel on hub causes RP reset on hub router.

  Workaround: None

- CSCtb89767

  When the FP20 svti ipsec setup with 1 tunnel has been configured the ipsec part of the svti topology will be deleted; and re-configing the IPsec does not happen.

Workaround: Reload the router.

- CSCtc02012

  When using GETVPN with authentication based on preshared keys rhe KS sends, as ID payload in Main Mode 6, protocol 17 [udp] port 500 instead of protocol 17 [udp] port 848.

  Workaround: None

- CSCtc25464

  After the ASR 1000 Router Series has been reloaded, and the tunnel interface has been configured with keepalives it will remain in the line-protocol down state. This will occur only when keepalives are configured for a short interval (total timeout under 10 seconds) and when the box has been reloaded.

  Workaround: Is to remove the keepalive configuration on the tunnel and to reload the configuration again; after the router has rebooted when the tunnel interface is still down.

- CSCtc38036

  The file table overflow error will occur when the file system is being accessed. This will occur after a few days on the ASR 1000 Router Series when running 2.4.1 and 2.4.2:

  router#more system:running-config

  %Error opening system:running-config (File table overflow)

  Workaround: Reloading the router solves the problem, but it appears again after a few days.

- CSCtc38484

  The giga word counters are not reflecting properly in the stop record.

  Workaround: There is no issues when the interim record is enabled. When the interim accounting is disabled on the ASR 1000 router, execute the **show interface virtual** command. This will allow for the giga word counter in the stop record to be confiigured.

- CSCtc40677

  When the distribute list is applied to the virtual template the distribute-list applied to the virtual-template interface is not effective for the virtual-access interfaces spawned by that template.For example, when the ASR 1000 router (hub) is configured as:

```
router eigrp 1
 redistribute static metric 10000 100 255 1 1500
 network 10.0.0.0
 no auto-summary
 distribute-list prefix TEST out Virtual-Template1!
ip route 0.0.0.0 0.0.0.0 Null0
ip route 10.0.0.0 255.0.0.0 Null0!
ip prefix-list TEST seq 10 permit 0.0.0.0/0
ip prefix-list TEST seq 20 permit 10.0.0.0/8
```

  For example:on the branch site when connected to a Virtual-accessinterface will show as:

```
ranch#sh ip route eigrp
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, *15:56:44.397 BRU Wed Oct 7 2009
10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D       10.0.0.0/8 [90/46251776] via 10.12.0.2, 00:00:06, Dialer1
D       10.1.1.0/24 [90/46228736] via 10.12.0.2, 00:00:06,Dialer1
D       10.2.2.0/24 [90/46354176] via 10.12.0.2, 00:00:06, Dialer1
D*EX 0.0.0.0/0 [170/46251776] via 10.12.0.2, 00:00:06, Dialer1
```

  For example: note that there is no filtering applied.

  In rare conditions this error may have occurred on the ASR 1000 router (hub) running 12.2(33)XND1 or later releases.

Workaround: Is to configure the distribute-list for the specific virtual-access interface used for the connections on the hub.

- CSCtc45743

  When VPN is configured between two ASR 1000 routers the traffic is encrypted, however when it reaches the end of the tunnel it is not decrypted. The flowing debug output is expected from “debug crypto ipsec”

  The IPSec configuration: (crypto_ipsec_create_transform_sas): Failed to attach flowid to hw

  In rare conditions this error may appear when the VPN tunnel has been created between two ASR 1000 routers on the RP2's and ESP20's running 2.4.1 and 2.4.2.

  Workaround: Reloading the router solves the problem,

- CSCtc45832

  When tracking stops the data-plane logs out of the PKT-MEM trace log this problem will occur on the ASR 1000 Router Series the sessions will be dropped and the QoS hierarchy will shut down. There also will be pending queue objects waiting to be flushed out in the list.

Note The following command will show the BQS RM status:

show plat hard qfp act inf bqs stat

In rare conditions, an error may occur for extreme over-subscribed enviroments. When sending 10G (For example: 5G as priority, and 5G as non-priority) traffic to a 1G interface.

All priority and control packets are dropped by the hardware this occur when the packet buffers are depleted; and when the schedule stops forwarding output packets

Workaround: There is no known workaround to this problem.

- CSCtc51048

  On the Cisco ASR 1000 Router the FP will reset, when configuring **show platform hardware cpp feature ipsec spd all** on the cli, after deleting tunnels FP crash on **sh pla hard cpp feature ipsec spd all** while deleting tunnels. This condition will occur when tunnel has been deleted and applyed to the CLI **show platform hardware cpp feature ipsec spd all** both even should happen together.

  Workaround: Do not apply CLI **show platform hardware cpp feature ipsec spd all** while you are deleting number of tunnels.

- CSCtc59162

  When modifying the prefix-list when configured as an inbound or outbound distribute-list does not trigger a resync of the EIGRP peer. This condition happens whe the Prefix-list has been has EIGRP as an inbound or outbound distribute-list.

  Workaround: To soft: clear the neighbor; and soft: clear ip eigrp neighbor <INTF_NAME>.

- CSCtc72899

  On the ASR 1000 Router Series does allow for abbreviated interface names this should be accepted by platform commands.

  Workaround: None

- CSCtc75736

  When EIGRP is configured on the ASR 1000 Router Series the MVPN Hub role stops sending acknowledgements for reliable packets. This condition on occurs when GRE Multipoint Tunnel shut/no shut has been applied.

Workaround: None

- CSCtc86951

  On the ASR 1000 Router Series, when high speed logging is enabled for NAT, ESP may fail after a RP SSO switchover. In rare conditions when high speed logging is enabled for NAT, ESP may fail after a RP SSO switchover.

  Workaround: None

Resolved Caveats—Cisco IOS XE Release 2.4.2

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.4.2

- CSCsc91697

  When DBS is applied Values (such as PCR, SCR and MBS) are not synced to standby. In rare conditions, an error will occur when DBS applied Values (such as PCR, SCR and MBS) are not synced to standby

  Workaround: None

- CSCse53019

  The BGP prefixes that should be redistributed to an IGP are not redistributed. When a route-map is used on the redistribution from BGP to the IGP and in the route-map statements such as **'match as-path...'or 'match community**..'are used to deny/allow networks to be redistributed. The network is initially received by BGP with an as-path/community that is denied by the route-map and later on the as-path/community changes which should allow it through the route-map but this never happens. The other way around is also affected, thus initially the BGP prefix being allowed but then later having a prefix in the BGP/routing table that should NOT be redistributed in the IGP but is being redistributed.

  Workaround: Is to'clear ip route <prefix>' or 'clear ip route * ' will trigger redistribution checking. Alternatively BGP table maps can be used to set tag and to redistribute based on tag and not on as-path/community.

  Further Problem Description: When certain attributes such as as-path or communities for an existing BGP prefix change, the routing table is updated but redistribution is never called so if redistribution from BGP to IGP's is based on a route-map which uses match community/match as-path statements then they will never be re-evaluated. This can lead to routing loops or blackholes.

  Workaround: None

- CSCsq03955

  On the ASR 1000 Router Series there are certain comands, such as **show platform hardware qfp act stat drop | ex _0_,** when executed on the newly active FP after the previously active FP was removed, may crash the smand process. The smand process crash does not result in the router crashing.

  When the RP is configured it resets to do shut/no shut on mlppp interfaces. This conditions occurs when s**hut/no shut** on mlppp interfaces, RP is reset on the ASR 1000 Router.

  Workaround: None

- CSCsq11897

  When BGP is configured on the ASR 1000 Router Series the system will crash when the interface board is removed. This rare condition is when BGP session is established and the corresponding interface board is removed.

Workaround: None

- CSCsr88898

  When spurious memory access may occur for scaled ppp sessions. In rare conditions an spurious memory access seen on clearing l2tp tunnel with scaled ppp sessions happens.

  Workaround: No workaround

- CSCsu46644

  When the ASR 1000 Router Series has rebooted you will no longer recieve username/password prompt until standby RP reaches SSO mode. The msg **%authentication failed** is received instead of router login prompt.

  Workaround: Add **no aaa account system guarantee-first** configuration.

- CSCsu52800

  When vrf configured has been configured (more than 1000 in this case), MCASTRED-3-DDE_REPLAY_FAILSAFE error message is displayed.

  Workaround: Is to increase the timeout of the PIM NSF Data Driven Event failsafe timer to resolve the problem.

- CSCsu82879

  After L4 redirect to broadhop SME portal, and with multiple subscribers trying to login into web server, the ASR1000 will popup with the following traceback:

  *Sep 29 11:11:40.830: %AAA-6-BADHDL: invalid hdl AAA ID 0, hdl 36020B6A, retired -Process= "SG CMD HANDLER", ipl= 0, pid= 151

  -Traceback= 1#afef50968b0f2116fc04276aae0dfa03 :10000000+50CA84 :10000000+50AC9C :10000000+50AF6C :10000000+40EB7C :10000000+418E98 :10000000+7E13A4 :10000000+7E125C :10000000+283889C :10000000+2833B64 :10000000+28353F0

  Workaround: None

- CSCsv91587

  The **aaa authorization** command, the **aaa authorization network default if-authenticated** only one session is coming up. The user receives authorization failures on the cli once log onto a device on the TACACS server; it is unreachable when logged in with their local credentials.

  Workaround: As the issue is specific to "if-authenticated" part in aaa authorization configuration [aaa authorization exec default group tacacs if-authenticated], the following configuration could be used as a workaround: [aaa authorization exec default group tacacs local]

- CSCsw31028

  The file type is mismatched in "show slot0:" and "show file info" output and the incorrect file type has been displayed for unicode file in show slot 0. This happens on the ASR 1000 Router Series when executing show slot0: it shows file type as config for unicode file.

  Workaround: None

- CSCsx06457

  The ASR 1000 Router Series when BGP is configured it may generate IPRT-3-NDB_STATE_ERROR log messages. An additional symptom when **bgp suppress-inactive** is configured is that the router CPU usage may get close to 100%. In rare conditions when both BGP and an IGP are advertising the same prefix, an error may occur. In addition **bgp suppress-inactive** command is configured with high CPU usage.

Workaround: Removing the **bgp suppress-inactive** configuration should eliminate the high CPU usage. Alternative option is to remove BGP or IGP conflicting routes from the system.

- CSCsx08861

  On the ASR 1000 Series the AToM VC status is seen as down in standby RP and traffic loss is seen after switchover for 44 seconds.

  Workaround: There are two work arounds for this issue:

  1. Do not reconfigure the ATOM VC immediately after deleting a subinterface.
  2. Do not copy and paste the ATOM VC

  Either do it manually step by step or copy the config from file.

- CSCsx29726

  On the ASR 1000 series router when the fail-close is unconfigured and the GDOI crypto map is in fail-close mode (after an unsuccessful registration), the crypto map will drop all unencrypted traffic regardless of a subsequent successful registration. On the ASR 1000 series router if fail-close is unconfigured when a GDOI crypto map is in fail-close mode (after an unsuccessful registration), the crypto map will drop all unencrypted traffic regardless of a subsequent successful registration. For this condition the symptom is observed when a GDOI crypto map configured with fail-close. Fail-close is unconfigured while crypto map is in fail-close mode.

  Workaround: Is to remove and reapply the crypto map to the interface or the fail-close configuration.

- CSCsx63700

  On the ASR 1000 Series the L2TP PMTU reset timeout, the Vaccess interface MTU is not restored to its original configured MTU. The old MTU value which was PMTU has been left on. On the ASR 1000 Serie this rare condition that will happen only on the VPDN LNS and when L2TP Path MTU is configured, and after a PATH MTU reset timeout.

  Workaround: None

- CSCsx90419

  ASR 1000 Router Series when policy is configured with excess bandwidth as well as queue-limit feature. In rare conditions when policy is confirgured on mfr interface the policy gets rejected instead of suspended.

  Workaround: None

- CSCsy07953

  On the ASR 1000 Series Router any attempt to copy a file from a router to an FTP server this will fail. On the FTP server the error is **No such file or directory.** For this rare condition the ASR 1000 Router Series has a problem with FTP when transferring files to an FTP server.

  Workaround: Is to use a different file transfer protocol, such as TFTP

- CSCsy08167

  On The ASR 1000 Router Series when auto re-enroll is started or a manual re-enroll is attempted for a certificate when Certificate Authority (CA) is using a manual grant method, the router will retry based on the default or configured retry counts and intervals. When the maximum retries are exceeded and the renewed certificate is not received from CA, the current certificate which is not yet expired, and this is not available until a reload.

  For the new IKE negotations using the **cypto pki authenticate ca** will fail with following message:

```
Feb 27 14:25:56.615: CRYPTO_PKI: Can't find signature certificate for
trustpoint
Feb 27 14:25:56.615: ISAKMP (7002): unable to build cert chain
```

```
Feb 27 14:25:56.615: ISAKMP (7002): FSM action returned error: 2
Feb 27 14:25:56.615: CRYPTO_PKI:
```

Workaround: There are two work around for this issue.

1. Is to increase the enrollment retries and count
2. Is to reload the router

- CSCsy16177

  On the ASR 1000 Series Router may experience invalid checksum over SCP on SSH version 2. This rare conditions may a occurs on a On the ASR 1000 Series Router with flash type file system.

  Workaround: There is no workaround.

- CSCsy19463

  On the ASR 1000 Series Router when NHRP has been configured as a mGRE tunnel interface configuration is related to NHRP/DMVPN the router may fail.

  Workaround: There is no workaround.

- CSCsy20343

  On the ASR 1000 Series Router may hang or bus error may cause a failure when polling CISCO-CLASS-BASED-QOS-MIB. In rare instances the ASR 1000 Router Series may fail when polling OID: 1.3.6.1.4.1.9.9.166

  Workaround: Is to Exclude OID: 1.3.6.1.4.1.9.9.166 or to disable SNMP.

- CSCsy22311

  When using secure copy (SCP) the ASR 1000 Router Series this may cause compatibility issues. In rare, conditions this may occur when using SCP SSH version 2 on the ASR 1000 Router Series.

  Workaround: None

- CSCsy33068

  On the ASR 1000 Series Router when the SDP HTML template are between 1KiB and 10KiB this may cause an abrupt termination of the SDP process. In rare instances the HTTP post to the HTTP server in an On the ASR 1000 Series Router is size-limited. The limit is set to 32KiB by default. In the SDP process, the transition from introduction page to the completion page involves an HTTP post. The post contains information including the SDP bootstrap configuration and the completion template together with the overhead of HTTP post communication. The size limit might be reached with moderate usage of HTML elements. The HTTP post in SDP is base-64 encoded. The total size limit of the SDP bootstrap and the completion template is roughly (32KiB - 2KiB(overhead))* 3/4(base-64 encoding) = 22.5KB.

  Workaround: Is to reduce the size of the HTML template, and abridge the configuration. The total size of the two cannot exceed ~22.5KB.

- CSCsy34538

  On the ASR 1000 Series Router after crypto PKI certiificate has been reloaded the certificates are not loaded from the USB Token when the reload of router certificates are not stored, or there not available on the Alladin USB token.

  Workaround: Is to copy certificate files from the usbtoken0: device into the nvram: filesystem and then configure **crypto pki certificate storage nvram.**

- CSCsy40745

When disabling SSH, an alternate SSH port this is still enabled on the ASR 1000 Series. This condition may occur on the ASR 1000 Series when has been configured to use a port other than Port 22 for SSH.

Workaround: Do not configure alternate SSH ports.

- CSCsy41887

  On the ASR 1000 Router Series an error message on console, or some traffic may drop when the ESP20 is configured for IPSec.

  Workaround: None

- CSCsy42850

  On the ASR 1000 Series Router when CNS is configure a memory leak may occur when using memory leak debug tool.

  Workaround: Is to not configure **cns**.

- CSCsy44755

  When IPv6 configuration is blocked when xconnect is configured for the interfaces on the ASR 1000 Router Series. This condition may be rare only when xconnect is configured for any interface on the ASR 1000 Router Series.

  Workaround: None

- CSCsy53445

  On the ASR 1000 Router Series the SDP server may fail on **crypto pki enroll <trustpoint>.**

  Workaround: None

- CSCsy79955

  On the ASR 1000 Router Series reverse SSH using PVDM2 modems may fail. If the **ssh -l <username>:<line #> <ip> command is entered,** and modem activation is triggered. The input of **atdt<number>** is making it to the modem, meaning whatever the <number> field is typed, it is reported in the debugs. However, the modem does not send anything back to router about it and no connection is made. At modem prompt, **at**, **at&f**, **ate1** (and perhaps others) do not appear to be taken.

  Workaround: Is to configure **ssh** (only)on the router,afterwards issue a **reverse** telnet

- CSCsy88034

  On the ASR 1000 Router Series the **flow data** in the **show ip cache [***verbose***] flow** commands output maybe missing. This condition may occurs when there is churn from netflow related configuration; especially exported configuration that are toggling **flow (enabling/disabling),** flapping of interface enabled with netflow.

  Workaround: Is to reload the router.

- CSCsy88764

  On the ASR 1000 Router Series the ISG PPPOE sessions may lose authenticated state if they receive Change of Authorization (COA) for service swapping. In rare instances when sending COA pushes to deactivate an existing service and active new one to ISG PPPOE sessions, the sessions may change state from authenticated to connect to the sessions that are already in logoff state. As a result, all Subscriber Service Switch (SSS) showings are empty.

  Workaround: None

- CSCsy90542

On the ASR 1000 Router Series the Multicast traffic is dropped at decrypting side. In rare conditions this symptom will occur when traffic ACL on the KS is of this type: permit **show ip host** *address* **show ip host** *any permit* **show ip host** *ip any host* **show ip host** *address* commands.

Workaround: There is no workaround.

- CSCsy92808

  On the ASR 1000 Router Series the certificate verification failure result is not returned to the client application(for opssl), instead a generic error is sent. This may be visible when SSLVPN and a connection to the back-end server is established via https, the page does not open and the browser hangs.

  Workaround: None

- CSCsy95838

  When external storage is configured on the ASR 1000 Router Series, the CRL may not be updated even if current CRL validity expires.

  Workaround: There are two workarounds for this issue:

  1. **shut/no shut** the crypto pki server.
  2. Increase the lifetime of CRL to maximum (2 weeks)
  3. Disable CRL checking

- CSCsy98000

  When IOS is configured on the ASR 1000 Router Series there maybe a failure when issuing **reload** command. In rare conditions, the ASR 1000 Router Series may fail on occasion if there are a large amount of messages that are to be printed on the IOS console.

  Workaround: Before reloading the router, disable console logging by giving the command **no logging console** from the configure mode. (or) Before reloading disable the watchdog issue the command **test platform software infrastructure watchdog off.**

  Instead of performing the above manual steps before each reload, please configure **logging reload errors** so that only more severe log messages are allowed to be printed on console during device reload.

- CSCsz02499

  When an Ethernet SPA interface with QinQ sub-interface configuration is disabled and then enabled, an error message about failing to apply PLIM input classification on the Ethernet SPA is displayed on the console. This condition is rare when QinQ sub-interface is configured on an Ethernet SPA on the ASR 1000 Router Series. The "show running-config" command is executed and then the Ethernet SPA interface is disabled and then enabled.

  Workaround: There is no functionality impact due to this error message. The QinQ sub-interface should be able to successfully pass traffic.

- CSCsz11759

  On the ASR 1000 Router Series the certificate enrollment process may fail for software crytpo engine.

  Workaround: None

- CSCsz22129

  On the ASR 1000 Router Series the class-maps in a QoS service-policy may get re-ordered by getting moved to the end of the policy-map. On the ASR 1000 Router Series this is arare condition the has been seen when the class-map is modified by adding new filters or modifying existing filters in the class-map.

Workaround: None

- CSCsz22367

  On ASR 1000 Router Series during a removal of BGP config with 'no router bgp' being copied from saved config file to running config.

  Workaround: None

- CSCsz26610

  On the ASR 1000 Router Series unexpected system reload may occur when "crypto pki authenticate CA" is configured with a certificate that is missing keyUsage = cRLSign. In rare instances when **crypto pki authenticate CA** command is configured with a certificate that is missing keyUsage = cRLSign a system reload may occur.

  Workaround: Is to configure "crypto pki authenticate CA" with a certificate that is includiing keyUsage = cRLSign.

- CSCsz27200

  Although the **show ip route** *ip-address* command is supported, the *ip-address* (or A.B.C.D.) option and its related parameters do not appear in the auto-completion list when the "?" or help prompt is entered for the **show ip route** command on a Cisco ASR 1000 Series Router.

  For example, note that the *ip-address* option does not appear in the list of subcommands below:

```
Router# show ip route ?
  bgp             Border Gateway Protocol (BGP)
  connected       Connected
  dhcp            Show routes added by DHCP Server or Relay
  eigrp           Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis            ISO IS-IS
  list            IP Access list
  loops           RIB routes forming loops
  mobile          Mobile routes
  multicast       Multicast global information
  odr             On Demand stub Routes
  ospf            Open Shortest Path First (OSPF)
  profile         IP routing table profile
  rip             Routing Information Protocol (RIP)
  static          Static routes
  summary         Summary of all routes
  supernets-only  Show supernet entries only
  topology        Display routes from a topology instance
  track-table     Tracked static table
  vrf             Display routes from a VPN Routing/Forwarding instance
  |               Output modifiers
```

  In addition, no list of optional parameters appear if the "?" or help prompt is entered following the **show ip route** *ip-address* command as shown below:

```
Router#sh ip route 10.1.1.1 ?
% Unrecognized command
```

  But the **show ip route** *ip-address* command is supported and works as expected:

```
Router#sh ip route 10.1.1.1
Routing entry for 10.1.1.1/32
  Known via "ospf 1", distance 110, metric 2, type intra area
  Last update from 10.0.0.3 on GigabitEthernet0/3/2, 4d01h ago
  Routing Descriptor Blocks:
    172.16.0.3, from 10.1.1.1, 4d01h ago, via GigabitEthernet0/3/2
      Route metric is 2, traffic share count is 1
```

```
  * 10.0.0.3, from 10.1.1.1, 4d01h ago, via GigabitEthernet0/3/0
      Route metric is 2, traffic share count is 1
Router#sh ip route 10.1.1.1 | in ospf
  Known via "ospf 1", distance 110, metric 2, type intra area
```

Workaround: None

- CSCsz45761

  When the SIP is configured on the ASR 1000 Router Series the messages can be dropped: - 200-OK - 183-SESSION-PROGRESS - 180-RINGING - ACK. In rare instances, the CONTACT header in the INVITE/200/183/180/ACK message may not have a port number specified on the ASR 1000 Router Series.

  Workaround: None

- CSCsz66842

  When Proxy service logon is configured it passes a wrong username on the ASR 1000 Router Series. In rare conditions the ASR 1000 Router Series when verifying the Tests for TC-Proxy, a service logon is performed with correct and incorrect username. When using incorrect Username, proxy service logon gets successfully applied as seen in the output of "show subscriber session all" even when Authentication gets rejected.

  Workaround: None

- CSCsz68932

  If a user enters an ambiguous command in adjacency sip submode on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) then the system leaves the prompt at the parent config-sbc-sbe level.

  For example, in the following sequence the user enters the ambiguous “re” command:

  ```
  Router(config-sbc-sbe)# adjacency sip client
  Router(config-sbc-sbe-adj-sip)# re
  % Ambiguous command:  "re"
  ```

  Now if the user tries to go back into the adjacency sip submode, the following error is displayed and the mode does not change:

  ```
  Router(config-sbc-sbe)#adjacency sip client
  Failed to access SBE cli configuration. Unable to execute command.
  ```

  Workaround: Exit the config-sbc-sbe submode to the config-sbc level. Then re-enter adjacency sip submode using the **sbe** and **adjacency sip** configuration commands as follows:

  ```
  Router(config-sbc-sbe)# exit
  Router(config-sbc)#sbe
  Router(config-sbc-sbe)#adjacency sip client
  Router(config-sbc-sbe-adj-sip)#
  ```

- CSCsz71478

  When there are a larger number of interfaces configured on the ASR 1000 Router the following traceback may appear:

  ```
  %AAA-3-BADLIST: invalid list AAA ID 11 -Process= "Exec", ipl= 0, pid= 76
  ```

  On rare conditions the trace-back may occur during boot-up time when there are a large number of interfaces configured on the ASR 1000 Router Series.

  Workaround: None

- CSCsz71654

When Accounting Records is configured on the ASR 1000 Router Series this may not show the correct username when the Web authenticated identifier uses IP addresses for routed IP sessions. In rare instances when on the ASR 1000 Router Series the account-logon (authentication) happens after failed Transparent Auto-Logon (TAL).

Workaround: None

- CSCsz72022

  The Cisco ASR 1000 Series Router crashes when a DBE command is entered on one line, and immediately after on another line, the SBC configuration is removed (for example, **no sbc** *name*). This text is similar to the following that is printed on the console, and then the router reloads.

  ```
  SBC: Assertion failed - csb->nvgen
  SBC: at ../sbc/sbc-infra/src/ios_cli/sbc_dbe_config.c:4323
  ```

  Workaround: Do not configure SBC on multiple lines simultaneously.

- CSCsz72973

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when malformed H.323 packets are received at a high rate and an Embedded Services Processor (ESP) switchover is in progress.

  This problem is intermittent

  Workaround: None

- CSCsz76450

  The Cisco ASR 1000 Router Series **show memory** *ip address* command may not allow for output.

  The console may return the following error message:

  % Invalid input detected at '^' marker

  In rare instances this may occur on a 64-bit Cisco ASR 1000 Router running in 2.3.0 or 2.4.0 releases.

  Workarond: None

- CSCsz77311

  Crash occurs in mfib_db_table_is_downloadable(). This issue may be seen when the following configuration command is issued:

  no ipv6 multicast-routing

  Workaround: None

- CSCsz91269

  The Cisco ASR 1000 Router Series may receive an error message return on the IOS console indicating a failure when downloading the correct NAT configuration from RP to CPP.

  This text is similar to the following that is printed on the console **ERR: %FMFP-3-OBJ_DWNLD_TO_CPP_FAILED: DYN-MAP: map_id 11 download to CPP"**

  Workaround: None

- CSCta00591

  The memory leak has been seen on the ASR 1000 Router Series when the router is configured to download lists or filters.

  Workaround: None

- CSCta06282

The Cisco ASR 1000 Router Series will do a check on whether the packet forwarding is working fine however there may be a rare instance when, the counters are not incrementing.

When turning on the **debug platform software multicast stat** this text is similar to the message n the console:

Jun 8 11:55:53.334: FMANRP-MCAST: M_ID 0 is not associated with an entry

The following message in this text that is similar to what may happen for special route combinations:

ipv6 mld static-group FF03::2:1:1

ipv6 mld static-group FF03::1:1:2

Workaround: To do group address changes.

- CSCta08194

  In rare instances the ASR 1000 Router Series may fail when reprovisioning AToM Tunnel with AAL5 Encapsulation.

  Workaround: None

- CSCta08772

  When EzVPN clients are failing negotiations on the ASR 1000 Router Series this may cause the router to use the less-specific route. In rare conditions the problem can occur when 0/0 is configured as a destination and EXACT_MATCH is specified.

  Workaround: None

- CSCta12296

  The Group Member crashes on the Cisco ASR 1000 Series Routers. In rare instances this occurs when unicast re-keys are received frequently (TEK 300).

  Workaround: None

- CSCta12360

  The Cisco ASR 1000 Series Router NAT Limit count may be falsely set to 0.

  This rare instance happens in lower traffic conditions when issuing **clear ip nat trans** after changing the limit maximum value.

  Workaround: Do not issue **clear ip nat trans** before changing maximum count for a limit.

- CSCta15960

  Spurious memory access followed by a traceback are logged on the ASR 1000 Series Router. In this rare condition the ASR 1000 Series Router is enrolling as a certificate server for the first time with GETVPN configured.

  Workaround: There is no workaround.

- CSCta22703

  The Cisco ASR 1000 Series Router has a problem that the 'agent address' field for coldstart and link down TRAP is notified as ip address of vlan1(shutdown).

  Workaround: To do snmp-server source-interface traps vlan "source vlan#" is set

- CSCta33240.

  CPP QoS EA encountered an error on the ASR 1000 Router Series. In this condition when an hierarchy policy-map is attached to the interface on both the input and output directions, after reloading the system by removing the policy-map without detaching it from the interface, an error message will occur on the console.

Workaround:Detach the policy-map from the interface then remove the policy-map.

- CSCta41084

  Packets encrypted and decrypted are not incrementing at the hub end after rekey. The issue is seen on a DMVPN head end aggregating 1000 spokes after the rekey timer has expired.

  Workaround: None

- CSCta57125

  Netflow statistics stopped updating after several instances of toggling between full and random sampled mode.

  Workaround: Do not toggle between full and random sampled Netflow mode.

- CSCta59045

  When the 32K dual stack sessions is configured on a PTA device (ASR1000 Series Router) with another ASR1000 client using the **test pppoe"**command, the client crashes with an IOS crash when 14K sessions comes up on the PTA. The ASR 1000 client crashes while in this condition, **test pppoe** command is configured, while trying to bring up 16K dual stack sessions on a PTA device and both the PPPoE client and PTA are ASR 1000 clients.

  Workaround: None

- CSCta63406

  In this condition when debug is used with **xconnect logging pseudowire status** the ADVIPSERVICESK9 image is unable to see **%XCONNECT-5-PW_STATUS** log message in the console.

  Workaround: None

- CSCta65367

  In this condition **show sbc** and **sbe call** commands will display call type as Audio.

  Work around: None

- CSCta65822

  When a switchover occurs on the ASR1000 Router Series for L2TP LAC thousands of sessions with tunnels are being disconnected, in some instances some sessions will be left in a "stale" state on the newly active RP. Apart from memory wastage, there is a functionality impact too future sessions with tunnels with the same session with tunnel ids as these stale sessions may be rejected.

  Workaround: Is to clear these stale sessions by using any clear commands. As a possible workaround is to ensure that all tunnels complete resync successfully by ensuring that either all sessions in it are not being disconnected at the same time that a switchover occurs OR by configuring "**l2tp tunnel timeout no-session <high value/never>"** on both LAC and LNS so that tunnel stays up even after there are no more sessions in it (so that it can complete successful resync).

- CSCta68936

  QoS VSA 1 attributes are not included in the service accounting record for complex QoS parameterized service.

  Work around: None

- CSCta72981

  In some conditions when creating a configuration view with **command parse view** this will not work, when **command configure** includes all **class-map type inspect.**

  Work around: None

- CSCta74405

When authentication is not configured in the transform-set, the output of IPSec SA shows anti-replay is disabled, but out of order packets are dropped once the default anti-replay window of 64 packets are reached.

Workaround: Is to disable anti-replay manually or increase the anti-replay window.

- CSCta86988

  The Cisco ASR 1000 Router Series will reload when using **debug sbc SBC-PE2 filter sip call** and **debug sbc SBC-PE2 filter call.**

  Workaround: Avoid enabling both debugs during critical call flow with this issue present.

- CSCta95969

  NAT pool address depletion occurs when running using PAT with pure IP traffic on the ASR 1000 Router Series.

  Workaround: Is to configure ACL to drop with pure IP traffic on NAT inside all interfaces.

- CSCta96311

  Decrypted IPSec packets are not forwarded to the IVRF with dual ISPs, when the primary default route has a higher number of interfaces with crypto mapping applied.

  Workaround: Is to use the command **no ip route-cache cef** on the ingress interface for incoming IPSec packet.

- CSCtb34308

  In rare conditions tracebacks are seen when initiating 4000 sessions on LNS on the Cisco ARS 1000 Router Series.

  Workaround: None

- CSCtc60363

  QoS queue-limit update does not work with qos fair-queue on the ASR 1000 Router Series, when configuring qos fair-queue and qos queue-limit in policy-map.

  Workaround: Is to change qos queue-limit before applying policy-map to interfaces.

Open Caveats—Cisco IOS XE Release 2.4.1

This section documents possible unexpected behavior by Cisco IOS XE Release 2.4.1.

- CSCse53019

  BGP prefixes that should be redistributed to an IGP are not redistributed.

  A route-map is used on the redistribution from BGP to the IGP and in the route-map statements such as ‘match as-path... or match community...' are used to deny/allow networks to be redistributed. The network is initially received by BGP with an as-path/community that is denied by the route-map. Later on the as-path/community changes which should allow it through the route-map but this never happens.

  The other way around is also affected. Thus initially the BGP prefix is allowed but then later having a prefix in the BGP/routing table that should *not* be redistributed in the IGP but is being redistributed.

  Workaround: The commands **clear ip route** *prefix* or **clear ip route *** will trigger redistribution checking. Alternatively BGP table maps can be used to set the tag and to redistribute based on the tag and not on as-path/community.

- CSCsw65614

Network Address Translation (NAT) is used with route maps with a SUP720 and some specific combinations of IP address, vlan# as outside interface, NAT for TCP application does not work correctly. With this issue, the extended VLAN is used for the outside interface, and the interface IP address matches the pool IP address.

Workaround: Use the **ip nat inside source route-map** *route-map* **interface** *interface* **overload** command as a substitute for **ip nat inside source route-map** *route-map* **pool** *pool* **overload** command.

- CSCsx61017

  Linecard switchover time is greater than expected. The error message is:

  ```
  error_msg = Switchover time is 70.631028 seconds, and expected is  1.5  seconds
  ```

  The issue occurs with all line cards. The issue is reproducible with a script only.

  Workaround: None

- CSCsx08861

  When an Any Transport over MPLS (AToM) virtual circuit (VC) subinterface is removed and then recreated (reprovisioned) on a Cisco ASR 1000 Series Router, the VC status on the standby RP should show as "HOTSTANDBY," but it shows as "DOWN." If a forced switchover is executed using the **redundancy force-switchover** command, the VC experiences about 44 seconds of traffic loss.

  Workaround: There are two possible workarounds for this issue.

  1. Do not reconfigure the AToM VC immediately after deleting the subinterface.
  2. Do not copy and paste the AToM VC configuration. Either do it manually step by step or copy the configuration from file.

- CSCsy19417

  When the number of Border Gateway Protocol (BGP) prefixes exceeds 300K in a Layer 3 VPN (L3VPN) scenario on a Cisco ASR 1000 Series Router and a reload is executed, Cisco Express Forwarding (CEF) is disabled. Before the reload, CEF functioned even though there were as many as 400K prefixes

  Workaround: None

- CSCsy49927

  The IOSd process restarts and returns the following error message:

  ```
  %Error opening tftp://202.153.144.25/hprem/rtr_crest.exp (Timed out)
  ```

  Workaround: None

- CSCsy73014

  On a Cisco ASR 1000 Series Router, the Internet Protocol Communications (IPC) RX flow control signals do not function properly. Traffic in excess of the IPC RX rising threshold will trigger the IPC RX STOP signal. However, when traffic levels drop below the falling threshold, the IPC RX START signal will not be sent.

  Workaround: None

- CSCsz01980

  Under very rare conditions, an RP1 on a Cisco ASR 1000 Series Router may experience an unexpected watchdog timeout during boot or shutdown and reload.

  Workaround: None

Following the reload, the RP1 works as expected.

- CSCsz18138

  Removing IPv4 or IPv6 addresses from VRF interfaces on a Cisco ASR 1000 Series Router results in traceback.

  Workaround: None

- CSCsz24683

  Shutting down subinterfaces configured with bidirectional forwarding detection (BFD) results in traceback.

  Workaround: None

- CSCsz24818

  When the **ip telnet source interface** command is configured to point at an interface that has an IPv6 address on a Cisco ASR 1000 Series Router, the RP resets.

  Workaround: Do not use the **ip telnet source interface** command.

- CSCsz25573

  When the pado delay parameter is configured under 4000 bba-groups on a Cisco ASR 1000 Series Router configured as an L2TP Access Concentrator (LAC), the following error message appears repeatedly at the router:

  ```
  %AAA-3-ACCT_LOW_MEM_UID_FAIL: AAA unable to create UID for incoming calls due to
  insufficient
  ```

  If the configuration is saved to NVRAM, the router reloads repeatedly after a reboot

  Workaround: If the pado delay configuration is only applied to 1000 bba-groups, the problem does not occur.

- CSCsz26610

  An unexpected system reload occurs when the **crypto pki authenticate CA** command is configured on a Cisco ASR 1000 Series Router with a certificate that is missing keyUsage = cRLSign.

  Workaround: Configure the **crypto pki authenticate CA** command with a certificate that includes keyUsage = cRLSign.

- CSCsz27068

  Under rare conditions, Open Shortest Path First (OSPF) may reset when the interfaces on a Cisco ASR 1000 Series Router are unconfigured in a very short interval.

  This condition is caused by a timing issue in OSPF.

  Workaround: None

- CSCsz27200

  Although the **show ip route** *ip-address* command is supported, the *ip-address* (or A.B.C.D.) option and its related parameters do not appear in the auto-completion list when the "?" or help prompt is entered for the **show ip route** command on a Cisco ASR 1000 Series Router.

  For example, note that the *ip-address* option does not appear in the list of subcommands below:

  ```
  Router# show ip route ?
    bgp             Border Gateway Protocol (BGP)
    connected       Connected
    dhcp            Show routes added by DHCP Server or Relay
    eigrp           Enhanced Interior Gateway Routing Protocol (EIGRP)
    isis            ISO IS-IS
    list            IP Access list
  ```

```
  loops           RIB routes forming loops
  mobile          Mobile routes
  multicast       Multicast global information
  odr             On Demand stub Routes
  ospf            Open Shortest Path First (OSPF)
  profile         IP routing table profile
  rip             Routing Information Protocol (RIP)
  static          Static routes
  summary         Summary of all routes
  supernets-only  Show supernet entries only
  topology        Display routes from a topology instance
  track-table     Tracked static table
  vrf             Display routes from a VPN Routing/Forwarding instance
  |               Output modifiers
<cr>
```

In addition, no list of optional parameters appear if the "?" or help prompt is entered following the **show ip route** *ip-address* command as shown below:

```
Router# show ip route 3.3.3.3 ?
% Unrecognized command
```

But the **show ip route** *ip-address* command is supported and works as expected:

```
Router# show ip route 3.3.3.3
Routing entry for 3.3.3.3/32
  Known via "ospf 1", distance 110, metric 2, type intra area
  Last update from 63.0.0.3 on GigabitEthernet0/3/2, 4d01h ago
  Routing Descriptor Blocks:
    63.0.0.3, from 3.3.3.3, 4d01h ago, via GigabitEthernet0/3/2
      Route metric is 2, traffic share count is 1
  * 36.0.0.3, from 3.3.3.3, 4d01h ago, via GigabitEthernet0/3/0
      Route metric is 2, traffic share count is 1
Router# show ip route 3.3.3.3 | in ospf
  Known via "ospf 1", distance 110, metric 2, type intra area
```

Workaround: The **show ip route** *ip-address* command actually is supported; its syntax just does not appear at the "?" or help prompt. For detailed information on the syntax for the **show ip route** *ip-address* command, see the following online documentation at Cisco.com:

http://www.cisco.com/en/US/partner/docs/ios/iproute/command/reference/irp_pi2.html#wp1015483

- CSCsz42939

  IOS crashes when the Cisco ASR 1000 Series Router has multiple interfaces configured with SPA-4XCT3/DS0/ SPA-2XCT3/DS0 SPA. Configuring multiple channel groups on SPA-4XCT3/DS0 SPA and performing a soft/hard OIR causes the router to crash. The router reloads.

  Workaround: None

- CSCsz47599

  The T3/E3 interface on a Cisco ASR 1000 Series Router does not come up after the router reloads.

  This condition is the result of a timing issue.

  Workaround: Execute a **shut/no shut** on the affected interface to bring the interface up.

- CSCsz54781

  Session interim accounting for PPP over X (PPPoX) sessions is not functioning in Cisco IOS XE Release 2.3.0 and later releases. When interim accounting is enabled on a per-session basis, no interim accounting updates get sent to the AAA server for PPPoX sessions.

  Workaround: None

- CSCsz56462

  The default behavior of the Cisco ASR 1000 Series Router is for the Cisco Discovery Protocol (CDP) to be disabled.

  Workaround: To enable CDP, include the **cdp enable** command in the configuration.

- CSCsz68932

  If a user enters an ambiguous command in adjacency sip submode on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) then the system leaves the prompt at the parent config-sbc-sbe level.

  For example, in the following sequence the user enters the ambiguous “re” command:

```
Router(config-sbc-sbe)# adjacency sip client
Router(config-sbc-sbe-adj-sip)# re
% Ambiguous command:  "re"
```

  Now if the user tries to go back into the adjacency sip submode, the following error is displayed and the mode does not change:

```
Router(config-sbc-sbe)#adjacency sip client
Failed to access SBE cli configuration. Unable to execute command.
```

  Workaround: Exit the config-sbc-sbe submode to the config-sbc level. Then re-enter adjacency sip submode using the **sbe** and **adjacency sip** configuration commands as follows:

```
Router(config-sbc-sbe)# exit
Router(config-sbc)#sbe
Router(config-sbc-sbe)#adjacency sip client
Router(config-sbc-sbe-adj-sip)#
```

- CSCsz72022

  The Cisco ASR 1000 Series Router crashes when a DBE command is entered on one line, and immediately after on another line, the SBC configuration is removed (for example, **no sbc** *name*). Text similar to the following is printed on the console, and then the router reloads.

```
SBC: Assertion failed - csb->nvgen
SBC: at ../sbc/sbc-infra/src/ios_cli/sbc_dbe_config.c:4323
```

  Workaround: Do not configure SBC on multiple lines simultaneously.

- CSCsz72973

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when malformed H.323 packets are received at a high rate and an Embedded Services Processor (ESP) switchover is in progress.

  This problem is intermittent

  Workaround: None

- CSCsz77311

  Crash occurs in mfib_db_table_is_downloadable(). This issue may be seen when the following configuration command is issued:

no ipv6 multicast-routing

Workaround: None

- CSCsz82587

  If Multi Protocol Label Switching Traffic Engineering (MPLS-TE) sessions come up or go down during online insertion and removal (OIR) on a Cisco ASR 1000 Series Router, the router may reload.

  Workaround: None

- CSCsz89484

  Blacklisting of a VPN does not take effect on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) for the following configuration:

  ```
  sbe
   blacklist vpn vpn-name
    reaason authentication-failure
     trigger-size 2
  ```

  The intended blacklisting action does NOT take effect because the trigger-period is NOT configured.

  Workaround: Configure the trigger-period using the **trigger-period** *num time-units* command.

- CSCsz94376

  When a very large number of calls are being processed through Cisco Unified Border Element (SP Edition) (CUBE) on a Cisco ASR 1000 Series Router and CUBE is deactivated and activated, an exception occurs and the router reloads.

  Workaround: None

- CSCta27191

  When using the command **upgrade rom-monitor filename harddisk:asr1000-rommon.XND.pkg** all for upgrading ROMmon, XND ROMmon failed to upgrade the RP1 board on 6RU(RP2) chassis.

  Workaround: None

- CSCta41084

  Packets encrypted and decrypted are not incrementing at the hub end after rekey. The issue is seen on a DMVPN head end aggregating 1000 spokes after the rekey timer has expired.

  Workaround: None

- CSCta45697

  When the total throughput of high priority and low priority IPsec traffic oversubscribed the encryption/decryption engine, high priority IPsec traffic is sometimes dropped.

  Workaround: Reduce the IPsec traffic bandwidth to below threshold.

- CSCta57125

  Netflow statistics stopped updating after several instances of toggling between full and random sampled mode.

  Workaround: Do not toggle between full and random sampled Netflow mode.

- CSCta37340

  The **show memory debug** command shows an increase in memory leaks at the IOSD ipc task as SPA modules are disabled/stopped one by one.

  Workaround: None

- CSCta74405

When authentication is not configured in the transform-set, the output for the IPSec Security Association (SA) shows anti-replay is disabled, but out-of-order packets get dropped once the default anti-replay window of 64 packets is reached.

Workaround: Disable anti-replay manually or increase the anti-replay window.

- CSCta76460

  IPSec EZVPN tunnels may be lost (not rekeyed properly) after a few rekey intervals.

  Workaround: Increase the rekey interval to the maximum to avoid the frequency of rekeying.

- CSCta86988

  The Cisco ASR 1000 Series Router crashed during Session Border Control (SBC) debug using a normal call.

  Workaround: None

- CSCtb01505

  While unconfiguring OSPF configurations, the Cisco ASR 1000 Series Router crashes with ospf_build_net_lsa.

  Workaround: None

- CSCtb01934

  System returns to ROMmon when booting IOS XE XND with a corrupted hard disk. If the filesystem on the hard disk is severely corrupted, IOS XE will fail to boot and return to ROMmon.

  Workaround: Booting an IOS XE XNC image will correct the filesystem errors, and any subsequent boot of IOS XE XND will be successful.

- CSCtb05335

  When tunnel protection IPsec is configured on a Generic Routing Encapsulation (GRE) tunnel, Label Distribution Protocol (LDP) session is flapping and the LDP neighborship on the GRE tunnel is going down.

  Workaround: To change tunnel protection, stop the traffic and then apply or remove tunnel protection.

- CSCtb05810

  When applying the **no distance** command, the summary-prefix disappears from the route table. When you check the ospfv3 database, the summary route exists.

  Workaround: Configure summary-prefix command again.

- CSCtb07984

  The Cisco ASR 1006 router acting as a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) failed to apply D2 QoS on the first two PPPoX sessions after every new reboot, but configures D2 QoS on all subsequent sessions.

  Workaround: LNS router configures D2 QOS on all subsequent sessions.

- CSCtb08490

  IPSecv6 tunnel fails to come up after tunnel protection is configured/unconfigured. The issue is seen when IPv6 traffic is flowing through the tunnel.

  Workaround: Stop the traffic before configuring/unconfiguring tunnel protection.

- CSCtb11807

Route Processor (RP) crash occurs when enablingIPv4 and v6 multicast routing and MPLS on the same interface. Multicast MPLS is not a supported mode for the Cisco ASR 1000 Series Router. The same interface requires all three features to be configured to cause the RP crash:

- IPv4
- IPv6
- MPLS
- ip sparse-dense mode

The following is a sample configuration:

```
interface GigabitEthernet0/3/2
 ip address 87.87.87.2 255.255.0.0
 negotiation auto
 ip sparse-dense mode   <<< will cause crash
 ipv6 address 2004:B010::6/64
 ipv6 ospf hello-interval 5
 ipv6 ospf 1 area 0
 mpls bgp forwarding
 cdp enable
end
```

Workaround: Do not configure MPLS on the same interface that uses IPv4 and IPv6 multicast since multicast MPLS is not a supported feature for Cisco ASR 1000 Series Router.

- CSCtb12998

  Not all calls are successful after RP switchover and **shutdown**, **no shutdown** of ingress interface.

  Workaround: You must reconfigure Session Border Control (SBC).

- CSCtb13472

  Label Distribution Protocol (LDP) session flaps between PE and P routers. There are 100 LDP targeted sessions between the PEs. When the targeted sessions flap, the link session between PE and P routers also flaps.

  Workaround: None

- CSCtb15399

  After prepaid (or possibly any service) download fails, the Cisco ASR 1000 Series Router crashes.

  Workaround: None

- CSCtb20400

  The Cisco ASR 1000 Series Router may crash when certain IPv6 crypto configurations are unconfigured when configurations are copied from the tftp to running config (**copy tftp: running-config**). The problem is not seen when the actual CLI is used (as opposed to **copy tftp: running-config**) on the router to unconfigure IPv6 IPsec. The problem also seems to be specific to RP2 since only the RP2 router has crashed so far, and it does not seem to affect RP1.

  Workaround: Use the CLI to unconfigure instead of configuring via the **copy tftp: running-config** command.

- CSCtb21280

  If billing is enabled with multiple instances as part of the Session Border Control (SBC) configuration, calls are processed by both instances for a short period of time and then an unexpected system reload occurs. This issue arises if billing records are being processed by a more than one billing instance.

Billing records are processed for both instances for a short time before an unexpected system reload occurs.

Workaround: At this time, using multiple billing instances leads to an unexpected system reload. Only a single billing instance can be used.

- CSCtb24845

  RADIUS throttling does not occur with a second server when there is a failover to the second server. Throttling happens for the first directed server but when there is a failover, the throttling does not happen.

  Workaround: None

- CSCtb27628

  A memory leak was observed when clearing crypto on a Cisco ASR 1000 Series Router.

  Workaround: None

- CSCtb28856

  On a Cisco ASR 1000 Series Router, in rare instances, with IP header compression (IPHC) configured, the Embedded Systems Processor (ESP) may unexpectedly reload.

  The reload of the ESP may occur when there is a high rate of traffic over an interface that is configured with IPHC and the number of configured IPHC compression-connections is lower than the number of actual flows/connections in the traffic stream.

  Workaround: Increasing the number of compression-connections will reduce the likelihood of the Embedded Systems Processor unexpectedly reloading.

- CSCtb29094

  With an ASR1002 uSBC with software redundancy, hitting no activate on billing for the second time will result in a system hang. The conditions under which this issue occurs are as follows:

  1. On a freshly rebooted router with SBC configuration
  2. Voice calls with CDR caching enabled bring down the radius server interface.

  Workaround: Don't do no activate again after the first no activate.

- CSCtb29156

  When the RADIUS remote Customer template is used on an MLNS router, MLNS brings up a session without VRF configuration. The PPPoX session is up and gets an IP address from the designated VPN Routing and Forwarding (VRF) pool.

  Workaround: Use the local Customer template and virtual private dialup network (VPDN) configuration.

- CSCtb30072

  With a 1K DMVPN spoke, if you un/re-configure tunnel protection several times and un/re-configure tunnel interface may reset both Embedded Services Processors (ESPs).

  Workaround: After unconfiguring a tunnel interface with 1K DMVPN spoke, wait for a few seconds before reconfiguring the same tunnel interface with same DMVPN configuration.

- CSCtb31090

  The active ESP resets after the active RP Switchover happens. This occurred with a scaled configuration of static virtual tunnel interfaces (VTIs) up to 2k and bi-directional traffic of throughput 3Gig. After the active RP Switchover and the new RP begins stabilizing, the active ESP resets.

  Workaround: None

- CSCtb31378

  Under certain circumstances for MPLS and multicast traffic, the forwarding plane may be unable to forward packets.

  Workaround: None

- CSCtb32037

  Traffic loss occurs during Fast Reroute (FRR) link protection in a network with 1000 TE tunnels configured for FRR during Boot up. This condition happened only when the tunnels were configured during Boot up. It did not happen when the tunnels were configured after the router was UP.

  Workaround: Configure tunnels after router has booted up.

- CSCtb32502

  With a 1K DMVPN spoke, un/re-config tunnel protection several times and un/re-config tunnel interface, RP resets.

  Workaround: Wait till all DMVPN session is up/down before next un/re-config tunnel. That is, do not un/re-configure tunnel when there are many sessions in transaction state.

- CSCtb32591

  Tunnel interfaces flap without any events as the SA's life timer expires. The tunnel goes down randomly while or when the SAs are recreated. This condition occurs with a scaled configuration of static VTIs very predominantly and with traffic (uni- or bi-directional).

  Workaround: None

- CSCtb34308

  Tracebacks are seen while initiating 4000 sessions on a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS). Tracebacks are seen when a service-policy is configured on the virtual-template and on the RADIUS profile with different names.

  Workaround: Use the same service-policy name on the Virtual-template and on the Radius profile.

- CSCtb37274

  If billing is enabled with a valid cache path as part of the SBC configuration, and records are being written to a removable device, such as a USB drive, and the device is removed from the router, an unexpected system reload can occur.

  This issue occurs if billing records are being written to a removable device and while operations are active, the device is removed from the router. Upon replacing the device and attempting to deactivate billing, an unexpected system reload occurs.

  Workaround: To avoid this issue, do not remove the device billing records are cached to while records are being processed.

- CSCtb38886

  The commands **show sbc** *name* **dbe signaling-flow stats** and **show sbc** *name* **dbe media-flow-stat** may display incorrect "Packet rate" value.

  Workaround: Ignore the "Packet rate" value in the **show** command output.

- CSCtb38954

  The issu runversion command failed on doing ISSU superpackage downgrade. On executing **issu runversion**, Switchover happened and a new active came up with the new image but then rolled back to the old image.

  Workaround: None

- CSCtb40440

  The Embedded Services Processor (ESP) may reset when applying a frame-relay map class on a channelized interface used as FR/PVC.

  Workaround: The following may cause the issue to occur:

```
interface Serial0/3/0.1/1/1/1:1
....
 frame-relay interface-dlci 16
   class <map-class-name>
```

  Use the following configuration instead of the preceding:

```
interface Serial0/3/0.1/1/1/1:1
....
 frame-relay interface-dlci 16
 frame-relay fragment 128 end-to-end
 service-policy input <service-policy-name-1>
 service-policy output <service-policy-name-2>
```

- CSCtb26955

  The following error message is displayed:

```
%CRYPTO-4-GM_REGSTER_IF_DOWN: Can't start GDOI registration as interface
FastEthernet1.2 is down
```

  However, the interface is not actually down, and so the registration should go thru. This issue occurs under the following conditions:

  1. Manually clear the rekey SA (**clear cry isakmp** *connid*)

  2) Wait for the re-registration to start.

  Workaround: Manual deleting of rekey SAs is not a valid thing to do. Using the command **clear cry gdoi** *group* or removing and adding the crytpo map works.

Resolved Caveats—Cisco IOS XE Release 2.4.1

All the caveats listed in this section are resolved in Cisco IOS XE Release 2.4.1.

- CSCsu32069

  The Cisco ASR 1000 Series Router reloads when Call Home tries to establish a secure http connection to a server. This problem is observed under the following conditions:

  - The Call Home profile has an http destination address pointing to a secure http server.
  - No certification authority has been declared (using the **crypto pki trustpoint** command) to be used by secure http connection.

- CSCsw16157

  A Cisco ASR 1000 Series Router using Open Shortest Path First (OSPF) and Multi Protocol Label Switching Traffic Engineering (MPLS-TE) may reload or operate incorrectly following changes to the configuration of MPLS-TE tunnel interfaces or OSPF. In some instances a configuration change may cause an immediate reload. In other instances, memory may be corrupted, resulting in problems later.

- CSCsw63003

  On a Cisco ASR 1000 Series Router functioning as a provider edge (PE) router, continuous Border Gateway Protocol (BGP) activity results in the increasing allocation of BGP path attributes and increasing memory usage. Because of the continuous BGP activity, existing path attributes are not being reused, and, as a result, the number of BGP path attributes allocated increases even when the number of routes is not increasing.

- CSCsy30653

  When you delete and then re-apply a policy-map that is already attached to an interface on a Cisco ASR 1000 Series Router, the Quality of Service (QoS) classification might not take affect.

- CSCsy34917

  When a SPA is stopped before an RP switchover and then restarted after the switchover, IPSec Internet Key Exchange (IKE) packets drop and the Next Hop Resolution Protocol (NHRP) fails to come up.

- CSCsy37179

  When deleting and adding Multi Protocol Label Switching Traffic Engineering (MPLS-TE) interface tunnels on a Cisco ASR 1006 Router, the primary RP reloads and forces a switchover.

- CSCsy45414

  Open Shortest Path First version 3 (OSPFv3) sessions on a Cisco ASR 1000 Series Router flap due to the expiration of the dead timer. This condition seems to occur after a reload of the router. Executing a multicast ping does not work from one end of the link. The first hello message seems to be received, but not the subsequent ones.

- CSCsy58115

  The Border Gateway Protocol (BGP) process on a Cisco ASR 1000 Series Router may stop freeing memory and hold increased amounts of memory over time. This condition occurs because some BGP neighbors that are not in an established state are exchanging prefixes.

- CSCsy91226

  On a Cisco ASR 1000 Series Router with IP interworking in Ethernet over MPLS over GRE (EoMPLSoGRE) and keepalive enabled on a Generic Routing Encapsulation (GRE) tunnel, ip irdp packets from the customer edge (CE) router get stuck in the interface input queue of the xconnect interface.

- CSCsz31984

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when parsing certain H.225 packets by the H.323 Application Layer Gateway (ALG). This condition may be caused by malformed H.225 packets with TCP fragmentation.

- CSCsz47599

  The T3/E3 interface on a Cisco ASR 1000 Series Router does not come up after the router reloads. This condition is the result of a timing issue.

- CSCsz54781

  Session interim accounting for PPP over X (PPPoX) sessions is not functioning in Cisco IOS XE Release 2.3.0 and later releases. When interim accounting is enabled on a per-session basis, no interim accounting updates get sent to the AAA server for PPPoX sessions.

  There are no known workarounds.

- CSCsz55618

  The SSS Manager on a Cisco ASR 1000 Series Router reports a memory leak when Change of Authorization (CoA) requests are used to turn a parameterized QoS service on or off. This condition is observed when the Cisco ASR 1000 Series Router is configured with PPP Terminated Aggregation (PTA) and terminates PPPoEoQinQ sessions.

- CSCsz70244

  When either the **radius-server directed-request restricted** or **radius-server directed-request restricted** command is configured on a Cisco ASR 1000 Series Router, the authentication fails.

- CSCsz77684

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads when firewall sessions are cleared using the **clear zone-pair inspect sessions** command in scaled scenarios. This condition is only associated with SIP sessions and when the SIP ALG requests many levels of sub-channels.

- CSCsz79403

  On a Cisco ASR 1000 Series Router, a Virtual Private Dialup Network (VPDN) failover does take effect with certain VPDN IP addresses. This condition occurs because two busy L2TP Network Server (LNS) IP addresses are detected. Because its busy timeout is set to 1 second, the L2TP Access Concentrator (LAC) gets stuck in a loop adding an IP address to the busy list in one second and removing the IP address from the list in the next second.

- CSCsz85306

  If Cisco Unified Border Element (SP Edition) is deactivated and activated multiple times on a Cisco ASR 1000 Series Router, an “Assertion failed” message appears on the console and the router reloads.

- CSCsz86631

  Within a few minutes of bringing up Intelligent Services Gateway (ISG) sessions and Session Border Controller (SBC) calls together on a Cisco ASR 1000 Series Router, an exception occurs and the router reloads.

- CSCsz92328

  None of the interfaces on a Cisco ASR 1000 Series Router come up after a stateful switchover (SSO) is performed on a configuration with self-signed certificates.

  This condition is observed under the following scenario:

  1. A Rivest, Shamir, and Adelman (RSA) self-signed certificate is generated on the router.

  2. The router is reloaded.

  3. An SSO is performed on the router.

- CSCsz94321

  When priority bandwidth and bandwidth remaining ratio are configured in a service-policy and the policy is enabled on an Any Transport over MPLS (AToM) virtual path (VP) on a Cisco ASR 1000 Series Router, some of the user-defined traffic classes are not guaranteed the configured bandwidth.

- CSCta01819

  Dynamically changing the session shape rate (parent shape rate) does not take effect with an IPv6 model F QoS over PPPoEoQinQ configuration on a Cisco ASR 1000 Series Router.

- CSCta04866

  When a malformed SIP message is received on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) (CUBE), traceback appears and the CUBE process reloads.

- CSCta05335

  Both the Active and Standby Route Processors (RPs) on a Cisco ASR 1000 Series Router reload during sustained traffic. This condition is observed with IPv4 calls running at 50 CPS that employ SIP INFO for Dual-Tone Multifrequency (DTMF) transport on both caller and callee.

- CSCta08805

  When a per-feature push to change the qos policy-map by a Change of Authorization (CoA) request is followed by a switchover on a Cisco ASR 1000 Series Router, the session policy-map is no longer functional after the switchover. This condition occurs because High Availability (HA) is not supported with per-feature push.

- CSCta10015

  A temporary failure to send an Internet Protocol Communications (IPC) log ACK message causes the Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router to no longer be able to receive configuration updates from the control-plane.

- CSCta11780

  Call Admission Control (CAC) and billing configurations are missing on a Cisco ASR 1000 Series Router after a double RP switchover (for example, if an RP1 to RP0 switchover is followed by an RP0 to RP1 switchover).

- CSCta11932

  On a Cisco ASR 1000 Series Router, Cisco Unified Border Element (SP Edition) only times out IPv4 end-to-end incomplete calls after it receives the media timeouts. The expected behavior is that incomplete calls will time out much sooner and at a more even rate (of 50 CPS). As a result, CUBE becomes congested. Eventually, CUBE may reach its max activating calls limit (which is 800 on an RP1), and stop accepting any new calls.

- CSCta14525

  On rare occasions, the SPA Interface Processor (SIP) card on a Cisco ASR 1000 Series Router repeatedly reloads on bootup, followed by reloads of other SIP cards and Embedded Services Processor (ESP) cards.

Open Caveats—Cisco IOS XE Release 2.4.0

This section documents possible unexpected behavior by Cisco IOS XE Release 2.4.0.

- CSCsu32069

  The Cisco ASR 1000 Series Router reloads when Call Home tries to establish a secure http connection to a server.

  This problem is observed under the following conditions:

  – The Call Home profile has an http destination address pointing to a secure http server. For example:

  ```
  destination address http
  https://172.17.46.17/its/service/oddce/services/DDCEService
  ```

  – No certification authority has been declared (using the **crypto pki trustpoint** command) to be used by secure http connection.

  Workaround: Configure a certification authority to be used by the secure http connection using the **crypto pki trustpoint** command.

- CSCsw16157

  A Cisco ASR 1000 Series Router using Open Shortest Path First (OSPF) and Multi Protocol Label Switching Traffic Engineering (MPLS-TE) may reload or operate incorrectly following changes to the configuration of MPLS-TE tunnel interfaces or OSPF. In some instances a configuration change may cause an immediate reload. In other instances, memory may be corrupted, resulting in problems later.

  To be exposed to this problem, a router must have MPLS TE tunnel interfaces that are announced to OSPF. Systems that do not run OSPF or that do not use MPLS-TE are not affected.

  Routers using MPLS-TE primary auto-tunnels are particularly vulnerable because those tunnel interfaces may be removed as a result of network topology changes as well as by modifying the running configuration.

  Routers using auto backup tunnels to provide fast reroute for static MPLS-TE tunnels do not have any extra exposure to this problem because while these backup tunnels may be removed due to topology changes, the static tunnel to the same destination will not be removed.

  Some of the configuration changes that may cause the incorrect behavior are as follows:

  – The router may reload when the following configuration commands are issued:

    Global configuration mode commands:

    * **no interface tunnel** *n*

    * **no router ospf**

    * **no mpls traffic-eng auto-tunnel**

    Interface configuration mode commands:

    * **no ip unnumbered**

    * **no ip address**

    Exec mode command:

    * **clear mpls traffic-eng auto-tunne**l

  – Removing the last MPLS-TE tunnel interface to a destination.

  - Removing an auto-tunnel configuration.
  - Removal of dynamically created auto-tunnel interfaces as a result of changes in the network topology.

  Normal UP/DOWN state changes of tunnel interfaces do not cause problems.

  Workarounds: The possible workarounds include:

  - To remove an MPLS-TE tunnel interface, first configure it down with the **shutdown** command in interface submode.
  - To remove an OSPF instance, first disable MPLS-TE for the instance by configuring the **no mpls traffic-eng area** *n* command in router ospf submode.
  - No workaround is available for MPLS-TE auto-tunnels.

- CSCsw63003 confirm as still showing Resolved

  On a Cisco ASR 1000 Series Router functioning as a provider edge (PE) router, continuous Border Gateway Protocol (BGP) activity results in the increasing allocation of BGP path attributes and increasing memory usage.

  Because of the continuous BGP activity, existing path attributes are not being reused, and, as a result, the number of BGP path attributes allocated increases even when the number of routes is not increasing.

  Workaround: Reload the router if low memory conditions are reached, or identify the root cause of the continuous activity and attempt to fix that cause if possible.

- CSCsx08861

  When an Any Transport over MPLS (AToM) virtual circuit (VC) subinterface is removed and then recreated (reprovisioned) on a Cisco ASR 1000 Series Router, the VC status on the standby RP should show as "HOTSTANDBY," but it shows as "DOWN." If a forced switchover is executed using the **redundancy force-switchover** command, the VC experiences about 44 seconds of traffic loss.

  Workaround: There are two possible workarounds for this issue.

  1. Do not reconfigure the AToM VC immediately after deleting the subinterface.
  2. Do not copy and paste the AToM VC configuration. Either do it manually step by step or copy the configuration from file.

- CSCsy19417

  When the number of Border Gateway Protocol (BGP) prefixes exceeds 300K in a Layer 3 VPN (L3VPN) scenario on a Cisco ASR 1000 Series Router and a reload is executed, Cisco Express Forwarding (CEF) is disabled. Before the reload, CEF functioned even though there were as many as 400K prefixes

  There are no known workarounds.

- CSCsy30653

  When you delete and then re-apply a policy-map that is already attached to an interface on a Cisco ASR 1000 Series Router, the Quality of Service (QoS) classification might not take affect.

  Workaround: Use a different policy-map name with the same QoS configuration.

- CSCsy34917

  When a SPA is stopped before an RP switchover and then restarted after the switchover, IPSec Internet Key Exchange (IKE) packets drop and the Next Hop Resolution Protocol (NHRP) fails to come up.

  There are no known workarounds.

- CSCsy37179

  When deleting and adding Multi Protocol Label Switching Traffic Engineering (MPLS-TE) interface tunnels on a Cisco ASR 1006 Router, the primary RP reloads and forces a switchover.

  For example:

```
interface Tunnel101
 ip unnumbered Loopback0
 ip ospf cost 65000
 tunnel destination 100.17.5.4
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng forwarding-adjacency
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth 2
 tunnel mpls traffic-eng path-option 1 explicit name PATH1
 tunnel mpls traffic-eng path-option 2 explicit name PATH2
 tunnel mpls traffic-eng path-option 3 dynamic
```

  This condition is observed after two to six delete/add cycles.

  Workaround: Limit the number of mass edits of tunnel interfaces.

- CSCsy45414

  Open Shortest Path First version 3 (OSPFv3) sessions on a Cisco ASR 1000 Series Router flap due to the expiration of the dead timer.

  This condition seems to occur after a reload of the router.

  Workaround: Perform a **shut /no shut** of the interface or a reload of the router. If you remove and add the OSPFv3 configuration on the interface, you can temporarily avoid this condition.

  Further Problem Description: Executing a multicast ping does not work from one end of the link. The first hello message seems to be received, but not the subsequent ones.

- CSCsy49927

  The IOSd process restarts and returns the following error message:

```
%Error opening tftp://202.153.144.25/hprem/rtr_crest.exp (Timed out)
```

  There are no known workarounds.

- CSCsy58115 onfirm as still showing Resolved

  The Border Gateway Protocol (BGP) process on a Cisco ASR 1000 Series Router may stop freeing memory and hold increased amounts of memory over time.

  This condition occurs because some BGP neighbors that are not in an established state are exchanging prefixes. The condition can be diagnosed by examining the out put of the **show process memory sort**, **show ip bgp sum**, and **show ip bgp vpnv4 all sum** commands. The output will show that the number of BGP attributes is increasing over time in relation to the BGP prefixes even though the number of paths remains approximately the same.

  Workaround: Remove the configurations related to the inactive neighbors (neighbors in the Idle or Active states.)

- CSCsy73014

  On a Cisco ASR 1000 Series Router, the Internet Protocol Communications (IPC) RX flow control signals do not function properly. Traffic in excess of the IPC RX rising threshold will trigger the IPC RX STOP signal. However, when traffic levels drop below the falling threshold, the IPC RX START signal will not be sent.

  There are no known workarounds.

- CSCsy91226

  On a Cisco ASR 1000 Series Router with IP interworking in Ethernet over MPLS over GRE (EoMPLSoGRE) and keepalive enabled on a Generic Routing Encapsulation (GRE) tunnel, ip irdp packets from the customer edge (CE) router get stuck in the interface input queue of the xconnect interface.

  There are no known workarounds.

- CSCsz01980

  Under very rare conditions, an RP1 on a Cisco ASR 1000 Series Router may experience an unexpected watchdog timeout during boot or shutdown and reload.

  There are no known workarounds. Following the reload, the RP1 works as expected.

- CSCsz18138

  Removing IPv4 or IPv6 addresses from VRF interfaces on a Cisco ASR 1000 Series Router results in traceback.

  There are no known workarounds.

- CSCsz23927

  When you configure both multicast sessions and Intelligent Services Gateway (ISG) sessions on a Cisco ASR 1000 Series Router, the router reloads and reports SYS-3-CPUHOG.

  Workaround: Do not configure streams with the destination address 224.1.1.44 (the multicast address.)

- CSCsz24683

  Shutting down subinterfaces configured with bidirectional forwarding detection (BFD) results in traceback.

  There are no known workarounds.

- CSCsz24818

  When the **ip telnet source interface** command is configured to point at an interface that has an IPv6 address on a Cisco ASR 1000 Series Router, the RP resets.

  Workaround: Do not use the **ip telnet source interface** command.

- CSCsz25573

  When the pado delay parameter is configured under 4000 bba-groups on a Cisco ASR 1000 Series Router configured as an L2TP Access Concentrator (LAC), the following error message appears repeatedly at the router:

  ```
  %AAA-3-ACCT_LOW_MEM_UID_FAIL: AAA unable to create UID for incoming calls due to
  insufficient
  ```

  If the configuration is saved to NVRAM, the router reloads repeatedly after a reboot

  Workaround: If the pado delay configuration is only applied to 1000 bba-groups, the problem does not occur.

- CSCsz26610

  An unexpected system reload occurs when the **crypto pki authenticate CA** command is configured on a Cisco ASR 1000 Series Router with a certificate that is missing keyUsage = cRLSign.

  Workaround: Configure the **crypto pki authenticate CA** command with a certificate that includes keyUsage = cRLSign.

- CSCsz27068

  Under rare conditions, Open Shortest Path First (OSPF) may reset when the interfaces on a Cisco ASR 1000 Series Router are unconfigured in a very short interval.

  This condition is caused by a timing issue in OSPF.

  There are no known workarounds.

- CSCsz27200

  Although the **show ip route** *ip-address* command is supported, the *ip-address* (or A.B.C.D.) option and its related parameters do not appear in the auto-completion list when the "?" or help prompt is entered for the **show ip route** command on a Cisco ASR 1000 Series Router.

  For example, note that the *ip-address* option does not appear in the list of subcommands below:

```
Router# show ip route ?
  bgp             Border Gateway Protocol (BGP)
  connected       Connected
  dhcp            Show routes added by DHCP Server or Relay
  eigrp           Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis            ISO IS-IS
  list            IP Access list
  loops           RIB routes forming loops
  mobile          Mobile routes
  multicast       Multicast global information
  odr             On Demand stub Routes
  ospf            Open Shortest Path First (OSPF)
  profile         IP routing table profile
  rip             Routing Information Protocol (RIP)
  static          Static routes
  summary         Summary of all routes
  supernets-only  Show supernet entries only
  topology        Display routes from a topology instance
  track-table     Tracked static table
  vrf             Display routes from a VPN Routing/Forwarding instance
  |               Output modifiers
```

  In addition, no list of optional parameters appear if the "?" or help prompt is entered following the **show ip route** *ip-address* command as shown below:

```
Router# show ip route 3.3.3.3 ?
% Unrecognized command
```

  But the **show ip route** *ip-address* command is supported and works as expected:

```
Router# show ip route 3.3.3.3
Routing entry for 3.3.3.3/32
  Known via "ospf 1", distance 110, metric 2, type intra area
  Last update from 63.0.0.3 on GigabitEthernet0/3/2, 4d01h ago
  Routing Descriptor Blocks:
    63.0.0.3, from 3.3.3.3, 4d01h ago, via GigabitEthernet0/3/2
      Route metric is 2, traffic share count is 1
  * 36.0.0.3, from 3.3.3.3, 4d01h ago, via GigabitEthernet0/3/0
      Route metric is 2, traffic share count is 1
Router# show ip route 3.3.3.3 | in ospf
  Known via "ospf 1", distance 110, metric 2, type intra area
```

  Workaround: The **show ip route** *ip-address* command actually is supported; its syntax just does not appear at the "?" or help prompt. For detailed information on the syntax for the **show ip route** *ip-address* command, see the following online documentation at Cisco.com:

  http://www.cisco.com/en/US/partner/docs/ios/iproute/command/reference/irp_pi2.html#wp1015483

- CSCsz31984

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when parsing certain H.225 packets by the H.323 Application Layer Gateway (ALG).

  This condition may be caused by malformed H.225 packets with TCP fragmentation.

  There are no known workarounds.

- CSCsz35479

  The Embedded Services Processor (ESP) reloads on a Cisco ASR 1000 Series Router when **shut/no shut** or soft online insertion and removal (OIR) is executed on an asynchronous transfer mode (ATM) interface that has Quality of Service (QoS) configured.

  This condition occurs when traffic is passing through the ATM interfaces at the time the **shut/no shut** sequence (or soft OIR) is performed.

  There are no known workarounds.

- CSCsz47599

  The T3/E3 interface on a Cisco ASR 1000 Series Router does not come up after the router reloads.

  This condition is the result of a timing issue.

  Workaround: Execute a **shut/no shut** on the affected interface to bring the interface up.

- CSCsz54781

  Session interim accounting for PPP over X (PPPoX) sessions is not functioning in Cisco IOS XE Release 2.3.0 and later releases. When interim accounting is enabled on a per-session basis, no interim accounting updates get sent to the AAA server for PPPoX sessions.

  There are no known workarounds.

- CSCsz55618

  The SSS Manager on a Cisco ASR 1000 Series Router reports a memory leak when Change of Authorization (CoA) requests are used to turn a parameterized QoS service on or off.

  This condition is observed when the Cisco ASR 1000 Series Router is configured with PPP Terminated Aggregation (PTA) and terminates PPPoEoQinQ sessions.

  There are no known workarounds.

- CSCsz56462

  The default behavior of the Cisco ASR 1000 Series Router is for the Cisco Discovery Protocol (CDP) to be disabled.

  Workaround: To enable CDP, include the **cdp enable** command in the configuration.

- CSCsz68932

  If a user enters an ambiguous command in adjacency sip submode on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) then the system leaves the prompt at the parent config-sbc-sbe level.

  For example, in the following sequence the user enters the ambiguous “re” command:

```
Router(config-sbc-sbe)# adjacency sip client
Router(config-sbc-sbe-adj-sip)# re
% Ambiguous command:  "re"
```

Now if the user tries to go back into the adjacency sip submode, the following error is displayed and the mode does not change:

```
Router(config-sbc-sbe)#adjacency sip client
Failed to access SBE cli configuration. Unable to execute command.
```

Workaround: Exit the config-sbc-sbe submode to the config-sbc level. Then re-enter adjacency sip submode using the **sbe** and **adjacency sip** configuration commands as follows:

```
Router(config-sbc-sbe)# exit
Router(config-sbc)#sbe
Router(config-sbc-sbe)#adjacency sip client
Router(config-sbc-sbe-adj-sip)#
```

- CSCsz70244

  When either the **radius-server directed-request restricted** or **radius-server directed-request restricted** command is configured on a Cisco ASR 1000 Series Router, the authentication fails.

  There are no known workarounds.

- CSCsz72973

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router may reload when malformed H.323 packets are received at a high rate and an Embedded Services Processor (ESP) switchover is in progress.

  This problem is intermittent

  There are no known workarounds.

- CSCsz77684

  The Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router reloads when firewall sessions are cleared using the **clear zone-pair inspect sessions** command in scaled scenarios.

  This condition is only associated with SIP sessions and when the SIP ALG requests many levels of sub-channels.

  Workaround: To avoid this problem before clearing firewall sessions set up access control lists (ACLs) on the interfaces where the SIP flows traverse. These ACLs should deny SIP control packets (port 5060). The sessions will time out based on the idle time configured by the firewall parameter maps.

  Further Problem Description: Firewall sessions are kept in a hierarchy. The numbers of levels in this hierarchy are limited. SIP violated this limit by requesting a hierarchy of sessions hundreds of levels deep. The firewall did not protect itself from this condition. When firewall sessions are cleared, the firewall recursively follows the hierarchy of a given session to tear down all the children and sibling sessions. Because there were hundreds of levels, the firewall exhausted the stack.

- CSCsz79403

  On a Cisco ASR 1000 Series Router, a Virtual Private Dialup Network (VPDN) failover does take effect with certain VPDN IP addresses.

  This condition occurs because two busy L2TP Network Server (LNS) IP addresses are detected. Because its busy timeout is set to 1 second, the L2TP Access Concentrator (LAC) gets stuck in a loop adding an IP address to the busy list in one second and removing the IP address from the list in the next second.

  There are no known workarounds.

- CSCsz82461

  When a **match-time** command is executed on a Cisco ASR 1000 Series Router after deactivating the Cisco Unified Border Element (SP Edition) and the corresponding call policy set, an "Assertion failed" message appears on the console and the router reloads.

  There are no known workarounds.

- CSCsz82587

  If Multi Protocol Label Switching Traffic Engineering (MPLS-TE) sessions come up or go down during online insertion and removal (OIR) on a Cisco ASR 1000 Series Router, the router may reload.

  There are no known workarounds.

- CSCsz85306

  If Cisco Unified Border Element (SP Edition) is deactivated and activated multiple times on a Cisco ASR 1000 Series Router, an "Assertion failed" message appears on the console and the router reloads.

  There are no known workarounds.

- CSCsz86631

  Within a few minutes of bringing up Intelligent Services Gateway (ISG) sessions and Session Border Controller (SBC) calls together on a Cisco ASR 1000 Series Router, an exception occurs and the router reloads.

  There are no known workarounds.

- CSCsz89484

  Blacklisting of a VPN does not take effect on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) for the following configuration:

  ```
  sbe
   blacklist vpn vpn-name
    reaason authentication-failure
     trigger-size 2
  ```

  The intended blacklisting action does NOT take effect because the trigger-period is NOT configured.

  Workaround: Configure the trigger-period using the **trigger-period** *num time-units* command.

- CSCsz92328

  None of the interfaces on a Cisco ASR 1000 Series Router come up after a stateful switchover (SSO) is performed on a configuration with self-signed certificates.

  This condition is observed under the following scenario:

  1. A Rivest, Shamir, and Adelman (RSA) self-signed certificate is generated on the router.

  2. The router is reloaded.

  3. An SSO is performed on the router.

  Workaround: After the reload, remove and add the self-signed certificate.

- CSCsz94321

  When priority bandwidth and bandwidth remaining ratio are configured in a service-policy and the policy is enabled on an Any Transport over MPLS (AToM) virtual path (VP) on a Cisco ASR 1000 Series Router, some of the user-defined traffic classes are not guaranteed the configured bandwidth.

  There are no known workarounds.

- CSCsz94376

  When a very large number of calls are being processed through Cisco Unified Border Element (SP Edition) (CUBE) on a Cisco ASR 1000 Series Router and CUBE is deactivated and activated, an exception occurs and the router reloads.

  There are no known workarounds.

- CSCta00666

  W hen the Session Border Controller (SBC) **activate** command is issued on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition), the RP reloads.

  This condition is observed with SBC calls running at 50 CPS.

  There are no known workarounds.

- CSCta01819

  Dynamically changing the session shape rate (parent shape rate) does not take effect with an IPv6 model F QoS over PPPoEoQinQ configuration on a Cisco ASR 1000 Series Router.

  Workaround: Do not change the shape rate dynamically. Remove the policy map before you the change the rate and then re-attach it with the new shape rate.

- CSCta04866

  When a malformed SIP message is received on a Cisco ASR 1000 Series Router configured with Cisco Unified Border Element (SP Edition) (CUBE), traceback appears and the CUBE process reloads.

  Workaround: Possible workarounds include:

  1. Use of SIP ports outside the standard 5060 range can help mitigate the possibility that an attacker can send malformed messages to the correct address and port.

  2. Blacklisting may help as well.

- CSCta05335

  Both the Active and Standby Route Processors (RPs) on a Cisco ASR 1000 Series Router reload during sustained traffic.

  This condition is observed with IPv4 calls running at 50 CPS that employ SIP INFO for Dual-Tone Multifrequency (DTMF) transport on both caller and callee.

  Workaround: Employ another means of DTMF transport such as RFC-2833.

- CSCta05882

  On a Cisco ASR 1000 Series Router, the Multicast Forwarding Information Base (MFIB) is not populated with the (*,G) and (S,G) entries when the **ip pim rp-address** command is configured with an access control list value.

  There are no known workarounds.

- CSCta08805

  When a per-feature push to change the qos policy-map by a Change of Authorization (CoA) request is followed by a switchover on a Cisco ASR 1000 Series Router, the session policy-map is no longer functional after the switchover.

  This condition occurs because High Availability (HA) is not supported with per-feature push.

  Workaround: To change the qos policy-map using a CoA, the service-policy should be present in either a user-profile (downloaded at authentication) or in a service-profile (downloaded at service logon).

- CSCta10015

  A temporary failure to send an Internet Protocol Communications (IPC) log ACK message causes the Embedded Services Processor (ESP) on a Cisco ASR 1000 Series Router to no longer be able to receive configuration updates from the control-plane.

  Workaround: Reload the ESP experiencing the problem.

- CSCta10764

  The Cisco Unified Border Element (SP Edition) SIP application on a Cisco ASR 1000 Series Router is not VRF-address aware when overlapping local ip addresses are used.

  Workaround: Use non-overlapping local ip addresses.

- CSCta11780

  Call Admission Control (CAC) and billing configurations are missing on a Cisco ASR 1000 Series Router after a double RP switchover (for example, if an RP1 to RP0 switchover is followed by an RP0 to RP1 switchover).

  There are no known workarounds.

- CSCta11932

  On a Cisco ASR 1000 Series Router, Cisco Unified Border Element (SP Edition) only times out IPv4 end-to-end incomplete calls after it receives the media timeouts. The expected behavior is that incomplete calls will time out much sooner and at a more even rate (of 50 CPS). As a result, CUBE becomes congested. Eventually, CUBE may reach its max activating calls limit (which is 800 on an RP1), and stop accepting any new calls.

  There are no known workarounds.

- CSCta12512

  Packets fail to get classified when the IPSec **qos-preclassify** command is configured on a Cisco ASR 1000 Series Router.

  Workaround: Re-apply the configuration, and the classification should take effect.

- CSCta14525

  On rare occasions, the SPA Interface Processor (SIP) card on a Cisco ASR 1000 Series Router repeatedly reloads on bootup, followed by reloads of other SIP cards and Embedded Services Processor (ESP) cards.

  Workaround: There are no known workarounds. The only means of recovery is to reload the router.

  Further Problem Description: The core file indicates the reload occurred in the emd (environmental monitoring) process.