



# Release Notes for Cisco ASR 1000 Series, Cisco IOS XE Amsterdam 17.3.x

---

**First Published:** 2020-03-04

**Last Modified:** 2023-03-26

## About Cisco ASR 1000 Series Aggregation Services Routers

The Cisco ASR 1000 Series Routers carry a modular yet integrated design, so network operators can increase their network capacity and services without a hardware upgrade. The routers are engineered for reliability and performance, with industry-leading advancements in silicon and security to help your business succeed in a digital world that's always on. The Cisco ASR 1000 Series is supported by the Cisco IOS XE Software, a modular operating system with modular packaging, feature velocity, and powerful resiliency. The series is well suited for enterprises experiencing explosive network traffic and network service providers needing to deliver high-performance services.

Cisco ASR 1000 Series Routers are available in this options:

- Cisco ASR 1001-X Router
- Cisco ASR 1002-X Router
- Cisco ASR 1001-HX Router
- Cisco ASR 1002-HX Router
- Cisco ASR 1004 Router
- Cisco ASR 1006 Router
- Cisco ASR 1006-X Router
- Cisco ASR 1009-X Router
- Cisco ASR 1013 Router

For more information on the features and specifications of Cisco ASR 1000 Series Routers, refer to the Cisco ASR 1000 Series Routers [datasheet](#).



---

**Note** The Cisco IOS XE 17.3 release is the last release in which subpackage upgrade is supported for the following platforms:

- ASR 1004
- ASR 1002-X
- ASR 1001-X
- ASR 1001-HX
- ASR 1002-HX

The [subpackage upgrade](#) for these platforms will not be supported from Cisco IOS XE 17.4 release. These hardware platforms continue to support software redundancy.

---



---

**Note** Some YANG models are not fully compliant with all the IETF guidelines. The errors and warnings shown while executing pyang with **--lint** flag is currently deemed to be non-critical as they do not impact the semantic of the models or prevent the models from being used as part of the toolchains. To determine the issues with the models, run the `check-models.sh` script with **--lint** flag enabled.

It is recommended to ignore LEAFREF\_IDENTIFIER\_NOT\_FOUND and STRICT\_XPATH\_FUNCTIONS errors types when running pyang for validation as they are non-critical errors and do not impact the YANG model functionality

---



---

**Note** When you upgrade from one IOS XE release to another, you may see `%Invalid IPv6 address` error in the console log file. To rectify this error, enter global configuration mode, and re-enter the missing IPv6 alias commands and save the configuration. The commands will be persistent on subsequent reloads.

---



---

**Note** Starting with Cisco IOS XE 17.3.x, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

The licensing utilities and user interfaces that are affected by this limitation include only the following:

- Cisco Smart Software Manager (CSSM),
  - Cisco Smart License Utility (CSLU), and
  - Smart Software Manager On-Prem (SSM On-Prem).
-

## New and Enhanced Software Features for Cisco IOS XE Amsterdam 17.3



**Note** The Cisco IOS XE Amsterdam 17.3.1a is the first release for Cisco ASR 1000 Series Aggregation Services Routers in the Cisco IOS XE Amsterdam 17.3.1 release series.

*Table 1: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE 17.3.x*

Feature	Description
Support for IP Multicast over UDL functionality for PIM	The unicast and multicast routing protocols forward data on interfaces from which they have received routing control information using a bidirectional link. However, some network links are unidirectional, where the physical send-only interface is on the upstream router and the physical receive-only interface is on the downstream router. To control routing information in these unidirectional environments, use the IP multicast over UDL functionality.
Support for openconfig-lldp 0.2.1	This release supports version openconfig-lldp 0.2.1 of LLDP protocol. No additional configuration is required.
Improved output for show ip nat pool command	The output of the <b>show ip nat pool</b> command is improved to display extra details.
Improved output for show diagnostic command	The output of the <b>show diagnostic</b> command now includes details of the serial number of the card in the slot.
Partial Configuration on CPE	This feature introduces limited support for following multicast modules in native operational YANG models: <ul style="list-style-type: none"> <li>• PIM</li> <li>• MROUTE</li> <li>• MFIB</li> </ul>

Feature	Description
<a href="#">Show platform software cef ipv4 feature-all command</a>	<p>This command displays CEF information from the following commands without having to run each command individually :</p> <ul style="list-style-type: none"> <li>• <b>show ip route &lt;network&gt; &lt;network mask&gt;</b></li> <li>• <b>show ip cef &lt;network&gt; &lt;network mask&gt; internal</b></li> <li>• <b>show adjacency &lt;adj_id&gt; internal</b></li> <li>• <b>show platform software ip rp active cef prefix &lt;network&gt;/&lt;mask_length&gt; detail</b></li> <li>• <b>show platform software adjacency rp active index &lt;platform_adj_id&gt;</b></li> <li>• <b>show platform software ip fp active cef prefix &lt;network&gt;/&lt;mask_length&gt; detail</b></li> <li>• <b>show platform software adjacency fp active index &lt;platform_adj_id&gt;</b></li> <li>• <b>show platform hardware qfp active feature cef-mpls adjacency handle &lt;cpp_handle_id&gt;</b></li> </ul>
<a href="#">BGP EVPN Route Reflector for Route Types</a>	<p>L2 Tenant Routed Multicast (L2 TRM) relies on new route types in the EVPN overlay to achieve the IGMP/MLD proxy functionality using the BGP route reflector with the following route types:</p> <ul style="list-style-type: none"> <li>• Selective Multicast Ethernet Tag Route (+6)</li> <li>• EVPN Multicast Join Synch Route (+7)</li> <li>• Multicast Leave Synch Route (+8)</li> </ul>
<a href="#">Policy-Based Routing support to categorise Office365 traffic for Direct Internet Access</a>	<p>To identify and differentiate Office 365 network traffic, Microsoft provides a web service to publish Office 365 endpoints and services. The Cisco Software-Defined AVC (SD-AVC) and Cisco Network-Based Application Recognition (NBAR) use this web service to improve first packet classification of Office 365 traffic to categorize it as as either “optimize or “non-optimize.”</p>
<a href="#">Show packet tracer command</a>	<p>The output of the show platform packet-trace command now includes additional trace information for packets either originated from IOSd or destined to IOSd or other BinOS processes.</p>
<a href="#">New cipher suites for IP ssh Client and Server Algorithm:</a>	<p>To configure the HMAC algorithm of HMAC-SHA2-256-ETM@openssh.com or HMAC-SHA2-512-ETM@openssh.com as a cryptographic algorithm for IP SSH client. These cipher suites can be used with the <b>ip ssh client algorithm mac</b> and <b>ip ssh server algorithm mac</b> commands.</p>
<a href="#">Advertisement of Loopback Prefix SIDs of a Border Router in Multiple ISIS Domains</a>	<p>A border router can advertise loopback interface prefixes and the associated prefix Segment Identifiers (SIDs) in multiple ISIS domains. With such an advertisement, the routers in each associated domain can communicate with the border router using the same prefixes and prefix SIDs.</p>

Feature	Description
<a href="#">BGP Best External Path with MPLS VPN Inter-AS Options B and C</a>	In autonomous Systems, you can configure border routers in MPLS VPN Inter-AS Option B and Inter-AS Option C deployments to compute the best external paths to PE nodes. The primary border router advertises best external paths to internal BGP (iBGP) peers as back-up paths so that if a link in a best path fails, traffic flows along the best external path.
<a href="#">Enable debug information for Multicast:</a>	The following debug commands are introduced to enable the debugging information for Multicast via ConfD/NetConf: <ul style="list-style-type: none"> <li>• <b>debug platform condition feature multicast controlplane level</b></li> <li>• <b>debug platform condition interface gigabitEthernet 0/0/1.2 ipv4 access-list mcast</b></li> <li>• <b>debug platform condition feature multicast dataplane v4mcast submode</b></li> <li>• <b>debug platform condition feature multicast dataplane v6mcast submode</b></li> </ul>

**Table 2: New and Enhanced Features for Cisco Unified Border Element (CUBE)**

Feature	Description
<a href="#">Support for Cisco ASR-1006</a>	The Cisco CUBE is supported on Cisco ASR 1006-X with RP3 and ESP 100.
<a href="#">Support for 100 VRFs</a>	The current support limit is 54 VRF instances on a CUBE box. This requires customers to purchase additional hardware to meet requirements. For deployments such as HCS support greater number of tenants per box, the limit of VRF instances is improved to 100 VRFs. This feature is also introduced on CUBE enterprise.
<a href="#">Dial Peer Binding with Live Traffic</a>	The Live Bind feature allows you to either change or add binding on a dial-peer that does not have any active calls, while other dial-peers with the same binding has active calls.
<a href="#">Media Proxy Multi-forking using SIPREC</a>	The SIPREC-based CUBE Media Proxy solution supports forking to multiple recorders.
<a href="#">OPUS Codec Negotiation</a>	Support is introduced for OPUS audio codec with CUBE.
<a href="#">TLS Server Name Indication (SNI) - RFC6066</a>	Support is introduced for Server Name Indication (SNI). SNI is a TLS extension that allows a TLS client to indicate the name of the server that it is trying to connect during the initial TLS handshake process.

Feature	Description
<a href="#">Consumption of INVITE with Replaces</a>	Currently, CUBE has a known limitation in handling re-INVITE with replace headers. With this feature, this limitation is addressed with CUBE consuming the INVITE with Replaces header and bridging the call dialogs appropriately. This feature enhancement is essential for interoperability of CUBE with Microsoft Teams.

## New and Enhanced Software Features for Cisco IOS XE Amsterdam 17.3.2

*Table 3: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE 17.3.2*

Feature	Description
<a href="#">Smart Licensing Using Policy</a>	<p>An enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use.</p> <p>With this licensing model, you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. Only export-controlled and enforced licenses require Cisco authorization before use. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date.</p> <p>Multiple options are available for license usage reporting – this depends on the topology you implement. You can use the Cisco Smart Licensing Utility (CSLU) Windows application, or report usage information directly to CSSM. A provision for offline reporting for air-gapped networks, where you download usage information and upload to CSSM, is also available</p> <p>For a more detailed overview on Cisco Licensing, go to <a href="https://cisco.com/go/licensingguide">https://cisco.com/go/licensingguide</a>.</p>

Feature	Description
<a href="#">Cisco DNA Support for Smart Licensing Using Policy</a>	<p>Cisco DNA Center supports Smart Licensing Using Policy functionality starting with Cisco DNA Center Release 2.2.2. The corresponding minimum required Cisco IOS XE Release for this platform is 17.3.2.</p> <p>Implement the “Connected to CSSM Through a Controller” topology to have Cisco DNA Center manage a product instance. When you do, the product instance records license usage, but it is the Cisco DNA Center that initiates communication with the product instance to retrieve and report usage to Cisco Smart Software Manager (CSSM) and returns the acknowledgement (RUM ACK).</p> <p>In order to meet reporting requirements, Cisco DNA Center provides ad hoc or on-demand reporting, as well as scheduled reporting options. Cisco DNA Center also provides workflows for the installation and removal of the Smart Licensing Authorization Code (SLAC) for a product instance, if applicable.</p> <p><b>Note</b> On the Cisco DNA Center GUI, you can generate a SLAC only for HSECK9 licenses, and only for certain product instances. See the <a href="#">configuration guide</a> for details.</p>

## New and Enhanced Software Features for Cisco IOS XE Amsterdam 17.3.3

Table 4: New Software Features in Cisco ASR 1000 Series Release Cisco IOS XE Amsterdam 17.3.3

Feature	Description
Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy	<p>SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM. Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. The product instance can be configured to <i>push</i> the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to <i>pull</i> the required information from a product instance at a configurable frequency. After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Offline and online options are available for synchronization between CSSM and SSM On-Prem.</p> <p>Minimum Required SSM On-Prem Version: Version 8, Release 202102</p> <p>Minimum Required Cisco IOS XE Version: Cisco IOS XE Amsterdam 17.3.3</p> <p>For more information, see <a href="#">Smart Licensing Using Policy for Cisco Enterprise Routing Platforms</a>.</p>

## Cisco Bug Search Tool

[Cisco Bug Search Tool](#) (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

## Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3

### Resolved Bugs for Cisco IOS XE Amsterdam 17.3

Caveat ID Number	Description
<a href="#">CSCvh24730</a>	PfRv3: Crash while Printing the Same TCA Message
<a href="#">CSCvi67613</a>	Protocol type for GRE header doesn't work consistently with "cts sgt inline" enable over auto-tunnel
<a href="#">CSCvo26639</a>	ASR 1000: All platforms having overrun drops after 24 hrs while traffic running at NDR



Caveat ID Number	Description
<a href="#">CSCvp24405</a>	Router crash after adding macsec reply-protection command on an interface
<a href="#">CSCvp79052</a>	vManage is not exhibiting the correct hostname of cEdge
<a href="#">CSCvp88044</a>	Performance Monitor crash
<a href="#">CSCvq42698</a>	Update "bandwidth remaining percent" doesn't take effective reliably on datapath
<a href="#">CSCvq70448</a>	Unable to create EOS choice root table at the moment of connect SDHSL circuit
<a href="#">CSCvq93850</a>	Passive FTP will fail when going over NAT and either client or server are off a SM-X-ES3
<a href="#">CSCvr42504</a>	ping is not working on port-channel after router reload
<a href="#">CSCvr48928</a>	Template push stuck on vManage Cluster when pushing new System IP to Edge router
<a href="#">CSCvr89957</a>	CFT crashed frequently
<a href="#">CSCvr93635</a>	flows not moving to unutilized link even after the hardthreshold
<a href="#">CSCvs02000</a>	%IOSXE-3-PLATFORM: R0/0: kernel: DMA: Out of SW-IOMMU space
<a href="#">CSCvs27907</a>	Ctrl+Z causes syntax error: unknown argument
<a href="#">CSCvs28073</a>	IOS-XE device has memory leak in linux_iods-imag
<a href="#">CSCvs29412</a>	x509 SSH authentication incorrect UPN value selected
<a href="#">CSCvs38028</a>	cEdge_Policy_regression: Service IPv6 ping is failing if the interface vrf forwarding is replaced
<a href="#">CSCvs42498</a>	NAT Alias not created for some configuration when using application redundancy
<a href="#">CSCvs43170</a>	[vManage] Firewall inspect/drop stat values are incorrect on device dashboard
<a href="#">CSCvs45107</a>	AnyConnect fails to reconnect when original session expires
<a href="#">CSCvs45215</a>	Some CLI typo "policing" not "policying"
<a href="#">CSCvs45388</a>	Failed to clear allocated ports for PAT after PAT CLI removal
<a href="#">CSCvs47682</a>	Router crashed when attempting to remove a nonexistent trustpoint from dspfarm profile
<a href="#">CSCvs48162</a>	Seeing IsecOutput drop for cEdge even though ip packet size is less than 1442.
<a href="#">CSCvs51630</a>	cEdge: 'security ipsec replay-window' needs to support 8192
<a href="#">CSCvs53749</a>	EVPN RMAC stale routes seen
<a href="#">CSCvs55489</a>	XE RII flaps with NAT64 w/o ipv4 route
<a href="#">CSCvs56559</a>	show crypto pki server shows wrong expire certificate date

Caveat ID Number	Description
<a href="#">CSCvs56721</a>	spoke-to-spoke PLR packets should not change the interface PLR status
<a href="#">CSCvs57212</a>	NGIO Lite is crashed when MT SMS with special characters (EMS) is received
<a href="#">CSCvs59402</a>	Random IPSEC drops on ESP200 with esp-gcm transform set
<a href="#">CSCvs60195</a>	ASR 1000 ucode crash after too many locks in ZBF pair setup
<a href="#">CSCvs60310</a>	Punt Policer rates not defined for multiple platforms
<a href="#">CSCvs61402</a>	CFLOW_INSERT ABORT errors continue to increment
<a href="#">CSCvs65950</a>	IOS PKI: P12 not generated on IOS Sub CA at rollover certificate generation
<a href="#">CSCvs66091</a>	XE SD-WAN Router SSH might get disabled followed by software reset and another reload
<a href="#">CSCvs70052</a>	ALG with NAT trigger a crash when a DNS writeback occurs
<a href="#">CSCvs75868</a>	esg:destination overwhelmed messages are seen on sending high rate TCP traffic leading to iosd crash
<a href="#">CSCvs78594</a>	NAT doesn't translate SIP header's original source for return traffic on 16.9.3 and 16.9.4
<a href="#">CSCvs81098</a>	Orthrus : With "sh hw-module subslot <> status" cli interface flapping
<a href="#">CSCvs81791</a>	Fix for kernel driver issue causing wake up for empty block, packet too large to process
<a href="#">CSCvs88686</a>	ISR4K / ASR / CBR8 crash in cpp_cp_svr due to watchdog timeout
<a href="#">CSCvs92239</a>	PnP always fails in both 17.2.1 throttle and 17.3.1.
<a href="#">CSCvs96344</a>	ASR 1000 : OIR after clock set doesn't save the time in RTC(recommit of CSCvr27554)
<a href="#">CSCvs96540</a>	SDWAN device admin-tech has empty "show running config" in /tech/ios file
<a href="#">CSCvs96719</a>	ASR 1000: Unicast DHCPREQUEST dropped when received on a EoGRE tunnel configured with VRF
<a href="#">CSCvs98586</a>	Skip SDWAN tunnel encapsulated packets in UTD DP and set inspected flag when skipping inspection
<a href="#">CSCvs99705</a>	PKI CLI - no warning that rsakeypair name starting from 0 (zero) is not working for cert regenerate
<a href="#">CSCvt01186</a>	Interface does down when "l2vpn xconnect" command is removed
<a href="#">CSCvt01532</a>	SD-WAN router running 16.10.3 crashes with cpp_cp_svr fault
<a href="#">CSCvt03869</a>	Router reloads due to crypto pki crl request <trustpoint-name> during get a fresh copy of CRL
<a href="#">CSCvt04864</a>	cpp_cp_svr fault and fman_fp_image fault on ASR 1002-x routers running 16.12.2r

Caveat ID Number	Description
<a href="#">CSCvt05373</a>	SDWAN device and vmanage is not in sync when manual software reset is done
<a href="#">CSCvt06296</a>	AVL tree still points to a tree node which has been freed
<a href="#">CSCvt06922</a>	hidden policies and classifiers IOS native yang model config from "show sdwan running-config"
<a href="#">CSCvt08357</a>	Time mismatch on sum of lapsed times from FIA Trace output
<a href="#">CSCvt09354</a>	Active RP running Polaris crash when standby running 3.X inserted
<a href="#">CSCvt10151</a>	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability UTD
<a href="#">CSCvt10499</a>	"Exporter Version" is not correct in the FNF cpp client exporter show command
<a href="#">CSCvt12245</a>	16.12.3 ZBFW-Mismatch in firewall stats between the device and vmanage
<a href="#">CSCvt13776</a>	TSN. prd17 image : Crash @ __be_socket_remove_event_buffer
<a href="#">CSCvt15167</a>	Cedge QOS Policy-Map on Parent Interface Maps Traffic to Wrong Queue When Traffic on Sub-Int
<a href="#">CSCvt15551</a>	Crash observed in QFP in ASR1001-X running 16.06.05 when GPM is running low
<a href="#">CSCvt19873</a>	ASR 1000:Router stops forwarding traffic with MPLS TE & FRR when member link of port-channel is shut
<a href="#">CSCvt21263</a>	Crash upon delete of virtual-access when virtual-template has "no tunnel protection ipsec initiate"
<a href="#">CSCvt21373</a>	unexpected reload in CPP ucode forced by nat 514 .
<a href="#">CSCvt21691</a>	VLAN1 is allowed on the trunk port even though it is not allowed in configurations of C111 interface
<a href="#">CSCvt28357</a>	Cloudexpress Symlinks missing for httping, timeout, nslookup utility in ASR1K
<a href="#">CSCvt28541</a>	XE SD-WAN : cflowd not working after re attaching template
<a href="#">CSCvt30545</a>	Probe reported 100% Loss for SaaS while network and configuration are all good.
<a href="#">CSCvt31561</a>	TBAR is not disabled in GM when it is disabled in KS
<a href="#">CSCvt33018</a>	MACsec 128/256 XPN on 40g/100g, stop passing traffic for one of AN and interface link flap seen
<a href="#">CSCvt33028</a>	Part of double encapsulated frames dropped with TunnelDecapTooManyTimes code reason
<a href="#">CSCvt33799</a>	Virtual address not reachable: "mac:0000:0c07:xxxx download to DP failed" for HSRP / VRRP over BDI.
<a href="#">CSCvt35947</a>	Duplicate ipv6 address while connecting to remote client

Caveat ID Number	Description
<a href="#">CSCvt40523</a>	GETVPN: KS 16.12.x - COOP switchover causes GMs to immediately use new TEK rekey
<a href="#">CSCvt46779</a>	Route export not working as desired during failover testing
<a href="#">CSCvt49705</a>	Device Crash observed with NAT and once there is traffic from outside
<a href="#">CSCvt52051</a>	IPsec tunnel is getting established for a backup NHS DMVPN hub
<a href="#">CSCvt52168</a>	SSH Process Thrash During Normal Operations
<a href="#">CSCvt52825</a>	Memory leak in SCCP TLS Client on unexpected deregister event
<a href="#">CSCvt53726</a>	Packet Duplication fails to duplicate packets in Cedge Devices
<a href="#">CSCvt54305</a>	Device crashed after Boost license expire
<a href="#">CSCvt57538</a>	IOSd crash due to Segfault in Crypto IKEv2 in ikev2_free_id
<a href="#">CSCvt59311</a>	ASR 1000 crash when modifying crypto keyring configuration
<a href="#">CSCvt65588</a>	FlexVPN IKEv2 Tunnel route removed after establishing new IKEv2 SA to another peer
<a href="#">CSCvt80422</a>	RTP-NTE to OOB DTMF Interworking Failure over BDI with Dot1q Tagging
<a href="#">CSCvt99461</a>	Remove duplicate license keyword from show platform software license command
<a href="#">CSCvu57682</a>	ASR1001-X 16GB: Kernel crashes repeatedly after upgrading from 16.12.2 to 17.2.1
<a href="#">CSCvu82189</a>	Enabling guestshell gives "float division by zero"
<a href="#">CSCvu89033</a>	Template push error due to NAT-MIB process helper traceback/warm restart

### Open Bugs for Cisco IOS XE Amsterdam 17.3

Caveat ID Number	Description
<a href="#">CSCvt32383</a>	ASR1000 / RP2 upgrade fails from 16.9.4 to the 16.9.5
<a href="#">CSCvt35331</a>	Console port goes unresponsive, reboot required to restore it.
<a href="#">CSCvt50136</a>	ASR 1000 - all Platform : Observing IpFragErr for EMIX traffic with basic IPSEC config
<a href="#">CSCvt70321</a>	Non-recurring summer-time IOSd config is incorrectly replicated to BinOS TZ environment
<a href="#">CSCvt75633</a>	It takes long until FlexVPN IKEv2 tunnel re-establishes when tunnel flaps
<a href="#">CSCvt79205</a>	ASR1001-X: 'show environment' is no longer monitoring R0 voltage sensors
<a href="#">CSCvt97086</a>	ESPx : CMAN-FP process crash for get_fpga_version API fails

Caveat ID Number	Description
<a href="#">CSCvt97326</a>	ASR 1000: harddisk usage is always zero in "show platform resource" for consolidated platforms
<a href="#">CSCvt97642</a>	MIP100 - Continuous %SCOOBY-5-SERIAL_BRIDGE_BLOCK_EVENT flooding on the console
<a href="#">CSCvu00804</a>	AnyConnect authentication fails when password contains "&" character
<a href="#">CSCvu06483</a>	Data consistency errors seen on configuring mac-sec on the underlay interface with ipsec configured
<a href="#">CSCvu06877</a>	Regression: vEdge2000 cannot exceed more than 65K NAT sessions over GRE or IKE IPsec tunnel
<a href="#">CSCvu26585</a>	"req plat software trace archive" fails with "STORAGE_TARGET: unbound variable Operation failed"
<a href="#">CSCvu30539</a>	Inbound CoPP policy causes outbound packets to fail to show up in EPC
<a href="#">CSCvu46417</a>	ASR1k crash when doing a FIB lookup
<a href="#">CSCvu53184</a>	cEdge - CLI should ask for confirmation of request software reset
<a href="#">CSCvu65369</a>	Link auto-negotiation fails between C1111-4P ES-4 switch module and Meraki MX100
<a href="#">CSCvu67351</a>	No traffic passing into the router on Everest or Fuji releases.
<a href="#">CSCvu67687</a>	Packet Drops when EPC is off and MTU is over 1500
<a href="#">CSCvu70249</a>	ASR1001X:SDWAN Default Throughput is not Scaling to Max supported
<a href="#">CSCvu73323</a>	AAR policy does not work properly after Poweroff/Poweron Cedge ISR4451
<a href="#">CSCvu75453</a>	ESP20 Rommon upgrade fails from 15.3(3r)S to 16.2(1r)
<a href="#">CSCvu77711</a>	Missing Mandatory Transform Type (ESN) in IKEv2 ESP Protocol
<a href="#">CSCvu81329</a>	sec policy pushing fail when remove L7 app from rule and action to drop
<a href="#">CSCvu82790</a>	SIP2: kernel: write adm1075 register at D3 failed rtn=-16 seen during SOAK run
<a href="#">CSCvu85056</a>	HTX memory hold increases, till a point, in longevity test
<a href="#">CSCvu89214</a>	IOS-XE+ZBFW+CUBE: One-way-audio. TCP 5060 is not recognized as SIP.
<a href="#">CSCvu92277</a>	Memory leak observed for FTM process leading to a device crash eventually.
<a href="#">CSCvu95098</a>	GETVPN group member drops traffic due to replay failure every 497 days
<a href="#">CSCvu95121</a>	Static NAT outside breaks locally generated TCP/UDP traffic
<a href="#">CSCvv00755</a>	Static ip is pingable before interface cell goes up/up
<a href="#">CSCvv00899</a>	Adaptive QoS history record LOCAL-LOSS is always 0 on ISR1000 platform

Caveat ID Number	Description
<a href="#">CSCvv01250</a>	IGMP reports are forwarded to mrouter port untagged regardless of which VLAN the group is in
<a href="#">CSCvv01497</a>	ASR 1000 ESP100 crash due to Deadlock
<a href="#">CSCvv01509</a>	Data policy `from-tunnel` is not programmed if `from-service` presented
<a href="#">CSCvv03229</a>	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
<a href="#">CSCvv05364</a>	ASR1001-HX, CCP crash due to invalid address accessed by DTL
<a href="#">CSCvv07867</a>	IOS-XE-SDWAN ISR4451-X/K9 - Performance Throughput lower than expected
<a href="#">CSCvv08341</a>	Netconf deleting wrong IKEv2 parameters
<a href="#">CSCvv08952</a>	FirewallNotInitiator drops with ZBFW for DIA traffic over Dialer interface with UTD enabled
<a href="#">CSCvv09565</a>	Cellular modem does not come up after router reload from "factory-reset all" command
<a href="#">CSCvv09651</a>	NAT packet drops with IN_US_V4_PKT_FOUND_IPSEC_NOT_ENABLED sub-code
<a href="#">CSCvv09707</a>	Secondary KS does not push new policy after merge if IPD3P is configured
<a href="#">CSCvv11071</a>	vManage is attempting to strip multiple LTE modem configs from ISR1000 and template push fails
<a href="#">CSCvv12398</a>	Packet Consumed Silently on ASR1001-X
<a href="#">CSCvv13444</a>	Forty gigabit ethernet link down after repeated HA SSO (switchovers) on 9800-80
<a href="#">CSCvv14263</a>	Day 0 Config Bringup after Power OFF/ON   C1121X-8PLTEP
<a href="#">CSCvv16597</a>	Upgrading to 16.9.5 breaks the xconnect functionality of forwarding Superior BPDUs in ASR1002-X
<a href="#">CSCvv16686</a>	Date field in "show crypto pki server <> cert" output is getting misaligned
<a href="#">CSCvv17346</a>	unexpected reload due to Crypto IKEv2 process
<a href="#">CSCvv17488</a>	Memory leak in iomd
<a href="#">CSCvv17730</a>	IP DHCP Snooping not working for the voice vlan
<a href="#">CSCvv18392</a>	Champion One 10 Gig SFP is not recognized by ASR-1001HX running SDWAN code,

## Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.2

### Resolved Bugs for Cisco IOS XE Amsterdam 17.3.2

Caveat ID Number	Description
<a href="#">CSCvv85766</a>	Memory leak upon ssh/scp connections to a router

Caveat ID Number	Description
<a href="#">CSCuz84374</a>	SPA modules on ASR1002-X/ASR1001-X does not get recognized under show platform
<a href="#">CSCvh24730</a>	PfRv3: Crash while Printing the Same TCA Message
<a href="#">CSCvp24405</a>	Router crashes after adding macsec reply-protection command on an interface
<a href="#">CSCvp88044</a>	Performance Monitor crash
<a href="#">CSCvq42698</a>	Update "bandwidth remaining percent" doesn't take effective reliably on datapath
<a href="#">CSCvr09310</a>	vManage should be able to work with cEdge banners in the same way as with vEdges
<a href="#">CSCvr42504</a>	ping is not working on port-channel after router reload
<a href="#">CSCvr76593</a>	Memory leak in CC-API_VCM and CCSIP_SPI_CONTROL
<a href="#">CSCvr85094</a>	Enabling Telemetry can cause router to crash.
<a href="#">CSCvs30625</a>	SRTP - RTP Crash on ASR with GCM Ciphers
<a href="#">CSCvs42075</a>	crash with shared-line command
<a href="#">CSCvs59402</a>	Random IPSEC drops on ESP200 with esp-gcm transform set
<a href="#">CSCvs63606</a>	Ping fails on hundred gig primary interface with FRR configured though MPLS traffic is not impacted
<a href="#">CSCvs70206</a>	CUBE DNS cache clear should be limited only to the matched connection id
<a href="#">CSCvs90555</a>	Template push fails when enabling ipv4 addr family on BGP ipv4 neighbor
<a href="#">CSCvs92677</a>	Crash when removing interface not running isis but has isis config
<a href="#">CSCvs96344</a>	ASR1000 : OIR after clock set doesn't save the time in RTC(recommit of CSCvr27554)
<a href="#">CSCvt01186</a>	Interface does down when "l2vpn xconnect" command is removed
<a href="#">CSCvt02567</a>	bgp crash @ bgp_db_ipstr2address when get bgp neighbor via bgp-oper yang
<a href="#">CSCvt12245</a>	16.12.3 ZBFW-Mismatch in firewall stats between the device and vmanage
<a href="#">CSCvt15007</a>	Unable to detach device from Integration Management
<a href="#">CSCvt16595</a>	IOS XE SDWAN routers experience slow memory leak over time in 'ncsshd' process
<a href="#">CSCvt16988</a>	Existing configuration on a cEdge could not be modified by a new template
<a href="#">CSCvt18190</a>	Router crash when doing 'show bgp ipv6 unicast summary'
<a href="#">CSCvt19472</a>	ASR 1000 crash at SSS manager sss_info_get_next_lem()
<a href="#">CSCvt19772</a>	Stackwise Virtual FMAN-RP IPC channel stuck (paused)
<a href="#">CSCvt21373</a>	unexpected reload in CPP ucode forced by nat 514 .

Caveat ID Number	Description
CSCvt33018	MACsec 128/256 XPN on 40g/100g, stop passing traffic for one of AN and interface link flap seen
CSCvt33799	Virtual address not reachable: "mac:0000:0c07:xxxx download to DP failed" for HSRP / VRRP over BDI.
CSCvt38466	SNMP TIMETICKS difference between sysUpTime vs ipslaEtherJAggStatsStartTimeId
CSCvt40021	Omp-tag is not being set via route-map configuration under bgp
CSCvt46635	Traffic is not getting optimized and it goes as PT connections on CSR router reload in 17.2.1
CSCvt54359	BGP config does not rollback if template push errors out
CSCvt57181	Leaf sends packets to a wrong BVI MAC of ASR GOLF routers
CSCvt58616	L2VPN Crash @ Process = XC Mgr
CSCvt58858	Incorrect CEF programming for local SVI
CSCvt60040	VPLS:MAC learning not happening on SSO
CSCvt60979	1731: ODN Policy for Global prefix still UP even after withdrawing global routes
CSCvt65588	FlexVPN IKEv2 Tunnel route removed after establishing new IKEv2 SA to another peer
CSCvt67752	Object (IPv6 ACL ) stuck in forwarding data plane. No ipv6 traffic goes towards the upstream router
CSCvt73592	missing/corrupt IOS-XE PKSC10 format
CSCvt74694	Cert validation failures seen for traffic after template push with SSL
CSCvt76409	Crash due to "Crimson flush transactions Process"
CSCvt78405	Code review: Just fire assert when we reach limit of counter
CSCvt89337	Incorrect Source IP when resolving DNS
CSCvt89441	IOS-XE device crashed with CGD shared memory corruption freed by FMAN-FP
CSCvt90424	CRC increasing on down int Te0/0/20
CSCvt94577	Incorrect CEF entry for LISP action signal-fwd
CSCvt98034	BGP communities: changes to route-map which sets BGP communities discards existing communities
CSCvu00280	RP3/ESP100/X: Traffic loss of over 1s at FP switchover (plain ipv4)
CSCvu21761	RAR: PADG and PADC are not being consumed properly. PPPoE session statistics are not matching.



Caveat ID Number	Description
<a href="#">CSCvu22003</a>	vManage FW dashboard doesn't show all matched applications
<a href="#">CSCvu22576</a>	Keepalive CLI needs to be unhidden for GRE tunnel
<a href="#">CSCvu23567</a>	RSP3: BGP crash seen on Stand by router when 100 BGP sessions are established.
<a href="#">CSCvu26678</a>	Some qos config lost during upgrade to 17.02
<a href="#">CSCvu26741</a>	Punt-Keepalive crash with lsmapi_lo_drv and container app traffic.
<a href="#">CSCvu27813</a>	Complete Traffic drop seen on Head Node Post configuring Binding SID on PFP Policy
<a href="#">CSCvu34381</a>	Packets are not dropped as expected in selfzone to zone vpn 0 firewall config
<a href="#">CSCvu52218</a>	Router crashes frequently on NBAR
<a href="#">CSCvu54786</a>	Crash on configuring a highest key identifier for OSPF authentication under an interface
<a href="#">CSCvu65669</a>	Traffic drop from branch overlay ping to service side without zp vpn1 to vpn1 when FW & IPS enabled
<a href="#">CSCvu66723</a>	Evaluation of CVE-2020-10188 - Cisco IOS XE Persistent Telnet
<a href="#">CSCvu70571</a>	SD-WAN router ASR1001-X crashes when object-group service configuration is added
<a href="#">CSCvu80644</a>	LSP Checksum error when default-info originate is configured
<a href="#">CSCvu87786</a>	CUBE Segmentation Fault @ sipSPIFreeOneSCB due to corrupt ccb
<a href="#">CSCvu89033</a>	Template push error due to NAT-MIB process helper traceback/warm restart
<a href="#">CSCvu99616</a>	Snort initiate reset and Failed to load - Real websites in Browser
<a href="#">CSCvv05893</a>	CUBE router crashed due to memory corruption in subscription control block
<a href="#">CSCvv05895</a>	ASR1001-X: Issue a cpld reset instead of reboot in kcrash
<a href="#">CSCvv13193</a>	Memory leak 'Admin group' with some triggers in ISIS
<a href="#">CSCvv16164</a>	RSVP TE is not working for broadcast interfaces due to CSCvu94532
<a href="#">CSCvv20380</a>	Removing and Adding Bulk ACL leads to Tracebacks and Error-Objects

#### Open Bugs for Cisco IOS XE Amsterdam 17.3.2

Caveat ID Number	Description
<a href="#">CSCvs87249</a>	DHCP Server configuration inn Vmanage Template for a Cedge change order of the DNS servers
<a href="#">CSCvt51568</a>	Unexpected Reload due to Sessmgr
<a href="#">CSCvt76844</a>	ASR1002-X ESP crash in multikey_hash_ager_tw_timer_to()

Caveat ID Number	Description
<a href="#">CSCvt85954</a>	IWAN routers ISR4K unexpected reload multiple times
<a href="#">CSCvu04160</a>	Unexpected Reload in Device Classifier Code due to Segmentation Fault
<a href="#">CSCvu27910</a>	Controller crashes when FNF is configured under physical interface
<a href="#">CSCvu41583</a>	Controller crashes when FNF is configured under physical/port-channel interface
<a href="#">CSCvv03229</a>	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
<a href="#">CSCvv11423</a>	Remote EID space prefix not installed in CEF when overlapping prefix exists as Local EID
<a href="#">CSCvv47691</a>	Reload: IOS-XE router crashing due to DN mismatch
<a href="#">CSCvv49841</a>	ASR 1002-HX crashes due to stuck threads.
<a href="#">CSCvv65068</a>	Crash after flexible netflow cache cleanup
<a href="#">CSCvv71238</a>	Sup reload with cpp-bqs fatal

## Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.3

### Resolved Bugs for Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
<a href="#">CSCuv97577</a>	Mishandling of dsmpSession pointer causes a crash
<a href="#">CSCvu23516</a>	Static routes pointing to interface tunnel not valid after tunnel's source interface flaps.
<a href="#">CSCvu32771</a>	IOSd Crash due to Segmentation fault at SISF Main Thread
<a href="#">CSCvv03229</a>	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
<a href="#">CSCvv09342</a>	Cloud Express probes fails when two default rules are present
<a href="#">CSCvv40006</a>	Traceback: IP SLA triggers INJECT_HDR_LENGTH_ER and INJECT_FEATURE_ESCAPE log message
<a href="#">CSCvv61770</a>	Crash seen in isis_sr_uloop_lspdb_dump with 'debug isis microloop' enabled
<a href="#">CSCvv64633</a>	BGP: advertised community list is malformed due to GSHUT community
<a href="#">CSCvv71775</a>	Cellular interface down/up frequently occurs with DoCoMo MVNO sim
<a href="#">CSCvv78028</a>	No responder-bytes from cEdge when UTD is enabled
<a href="#">CSCvv79273</a>	Router may crash when using Stateful NAT64
<a href="#">CSCvv88621</a>	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvv93925</a>	ASR 1000 Series crashes when ACL deleted following object-group modification
<a href="#">CSCvv94743</a>	Data Plane fails over L2TPv3 while disabling VLAN limit restrictions with ASR1002-HX
<a href="#">CSCvw06719</a>	Platform ipsec reassemble transit" tail-drops unencrypted IPv4 Fragments with specific payload
<a href="#">CSCvw06780</a>	DMVPN with ipv6 link-local address do not register to HUB
<a href="#">CSCvw09486</a>	Router might crash after apply a class-map in input direction with bandwidth percentage
<a href="#">CSCvw10972</a>	NAT64 ALG: Router crashes on nat64_process_token
<a href="#">CSCvw11902</a>	Passive FTP doesn't work with NAT
<a href="#">CSCvw16643</a>	Device Template failing to attach after changing few device variables
<a href="#">CSCvw19171</a>	Smart license registration through explicit mode proxy server
<a href="#">CSCvw22760</a>	MACSEC MKA stops forwarding data after every 3rd rekey
<a href="#">CSCvw23041</a>	Crash seen on Fugazi due to %CPPHA-3-FAILURE: R0/0: cpp_ha: CPP 0 failure Stuck Thread(s)
<a href="#">CSCvw30128</a>	"Sequence id not available" in ACL code after DNAC upgrade
<a href="#">CSCvw31389</a>	Pktlog functionality is broken
<a href="#">CSCvw32481</a>	EVPN Type-2 IP/MAC route is created for not-connected SVI
<a href="#">CSCvw33113</a>	Unexpected reload in NHRP when access to an invalid memory region
<a href="#">CSCvw34157</a>	APPNAV CFT Crashes
<a href="#">CSCvw37109</a>	Pseudowire interface may be unexpectedly removed from VFI on unrelated configuration change
<a href="#">CSCvw38433</a>	OMP-Agent Routes in EIGRP changes AD to 252 on non-SDWAN devices
<a href="#">CSCvw39383</a>	CPP ucode crash with fw_base_flow_create
<a href="#">CSCvw40079</a>	ASR 1000 Series crashes in ipv6 mgd timer code when removing vrf config
<a href="#">CSCvw41482</a>	SSH with Certificate authentication does not work after upgrade to 17.3.1
<a href="#">CSCvw47640</a>	ASR 1000 Seriesdoing KS role for GETVPN is sending malformed rekey packets
<a href="#">CSCvw47800</a>	HSL Export over VASI Interface causes Netflow v9 Template Flooding
<a href="#">CSCvw48800</a>	Unable to transfer 1500 byte IP packet when using BRI bundled Multilink
<a href="#">CSCvw54076</a>	[SIT]: BFD sessions not established between Edges, with UTD enabled

Caveat ID Number	Description
<a href="#">CSCvw55030</a>	Dynamic Nat pool "ip aliases" are not created on the device
<a href="#">CSCvw55658</a>	EPA-QSFP-1X100GE / IOS XE 17.3 / incorrect LED and link status
<a href="#">CSCvw56517</a>	LMR Unable to hear first seconds of audio
<a href="#">CSCvw57670</a>	ASR 1000 Series: Critical process plogd fault on rp_0_0
<a href="#">CSCvw57860</a>	Duplicate entries seen in MAC filter table.
<a href="#">CSCvw58560</a>	FlexVPN reactivate primary peer feature does not work with secondary peer tracking
<a href="#">CSCvw62284</a>	ASR1000 ISG: Crash when processing DHCP Request
<a href="#">CSCvw62805</a>	SDWAN ZBFW CPU punted traffic mishandling -- Out2In packet looped
<a href="#">CSCvw64559</a>	Throughput license grace period starts counting down after upgrade router software
<a href="#">CSCvw68171</a>	Duplicate Bytes & Packet when Q in Q is configured
<a href="#">CSCvw76715</a>	OpenSSL vulnerability (CVE-2020-1971) evaluation for IOS-XE
<a href="#">CSCvw77485</a>	Router may not send PIM Register message if RP is reachable over TE tunnel
<a href="#">CSCvw80173</a>	BGP AS-path prepend: cEdge won't update correctly better prepended route.
<a href="#">CSCvw84759</a>	Device is crashing after Device Access Policy is attached
<a href="#">CSCvw84883</a>	DDNS feature triggers crash on 16.X/17.X releases due to memory corruption
<a href="#">CSCvw86295</a>	Crash while configuring l2vpn evpn instance for VXLAN
<a href="#">CSCvx08852</a>	Not able to create VFI instances
<a href="#">CSCvx12686</a>	ACL: Crash triggers after 'clear ip access-list counters' is used with more than 1k ACEs
<a href="#">CSCvx19209</a>	ISIS crash in isis_sr_tilfa_compute_protection
<a href="#">CSCvx36844</a>	Control plane hitting EID prefix entry limit for MAC after upgrade

### Open Bugs for Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
<a href="#">CSCvv82322</a>	Link issue when using macsec
<a href="#">CSCvv99281</a>	BQS crash on PPPoE session churn overnight
<a href="#">CSCvw11607</a>	Crash in DSP causing an mcpcce-lc-ms core file
<a href="#">CSCvw67366</a>	ASR1002-X: Punt keepalive crashed due to bqs related interrupt
<a href="#">CSCvw80667</a>	Severe traffic disruption due to non-stop flapping of MACSEC enabled interfaces post RP3 switchover

Caveat ID Number	Description
<a href="#">CSCvw87256</a>	ASR 1000 Series cpp_cp_svr crash with frequent underlay route removal and tunnel source changed every 1 second
<a href="#">CSCvw89147</a>	Crash at the moment of calculating tcp header
<a href="#">CSCvw92643</a>	Netflow crash at fnf_ipv6_output_feature_final_internal with flow record on IPv6 IPsec tunnel.
<a href="#">CSCvx08118</a>	Bug to further address CSCvt08179 : QFP crash due to hardware interrupt
<a href="#">CSCvx24332</a>	ucode crash with firewall timer lock
<a href="#">CSCvx24707</a>	bgp-neighbor down when push banner configuration failure
<a href="#">CSCvx25680</a>	IOS-XE Memory Leak in SSS Manager
<a href="#">CSCvx26652</a>	Router crash observed when AppNav Cluster delete with service-insertion enabled on LAN interface
<a href="#">CSCvx32807</a>	False positive alarm: IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL Fan Tray Bay 1 Fan Tray Module Missing
<a href="#">CSCvx35902</a>	fman_rp: qos_hqf [L:1.0, N:0x3485061e18 ] (0p, 0c) download to FP failed resulting in a crash

## Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.4a

### Resolved Bugs for Cisco IOS XE Amsterdam 17.3.4a

Caveat ID Number	Description
<a href="#">CSCvv92064</a>	App-aware policy need to be honored when queuing is not set by localized policy
<a href="#">CSCvv95280</a>	Cisco 1001-X ASR may crash when ZBFW HSL(High Speed Logging) is configured
<a href="#">CSCvv99281</a>	BQS crash on PPPoE session churn overnight
<a href="#">CSCvw05211</a>	Pre-mature session deletion leading to churn and lower TPS at scale
<a href="#">CSCvw11607</a>	Crash in DSP causing an mcpc-c-ic-ms core file
<a href="#">CSCvw21378</a>	Cisco 1001-X ASR built-in Tengig interfaces' counters increasing continuously and port stay up/up w/o SFP
<a href="#">CSCvw52574</a>	Cisco 1000 Series ASR configured with 'no ip unreachable' sending ICMP Type 3 Code 13
<a href="#">CSCvw81572</a>	Multiple crashes cpp_cp_svr and qfp-ucode on 16.12.4
<a href="#">CSCvw88098</a>	cEdge crashes while running web traffic testing with security features enabled

Caveat ID Number	Description
<a href="#">CSCVw90220</a>	Crash at #12 0x00007f010f4cb9db in cpp_bqs_rm_yoda_get_flush_obj while subscriber bringup
<a href="#">CSCVw94434</a>	BQS crash seen at cpp_qm_event_proc_defer_cb
<a href="#">CSCVw98579</a>	BQS crash seen in 17.3 while bringing up 30k PPPOE sessions
<a href="#">CSCVx02009</a>	cEdge running 17.3.2 crashed - Critical software exception / IOSXE-WATCHDOG: Process = SNMP ENGINE
<a href="#">CSCVx21270</a>	SDWAN custom policy that does not looked to be programmed correctly on the cedge platform
<a href="#">CSCVx23159</a>	FW-4-ALERT_ON: (target:class)-():getting aggressive seen when no half open feature configed
<a href="#">CSCVx32670</a>	Wrong reload reason reflected after a power outage.
<a href="#">CSCVx36146</a>	DCHP offer frame getting dropped on cEdge ISR4431 due to Policy
<a href="#">CSCVx36205</a>	Removing and Adding Bulk ACL leads to dataplane programming failure
<a href="#">CSCVx36763</a>	Zone Based Firewall on cEdge router dropping web traffic with the reason Zone-pair without policy
<a href="#">CSCVx44834</a>	Cisco 1000 Series ASR- ACE entry added after object-group is missing in hardware causing packets drops
<a href="#">CSCVx45788</a>	cannot apply ciscosdwan.cfg due to vpg-log-server-acl ACL on VirtualPortGroup0 for logging
<a href="#">CSCVx53049</a>	Crash when TPOOL is updating and 'wr mem' is issues at same time
<a href="#">CSCVx57615</a>	ZBFW blocking ACK packets for applications using cloudexpress SaaS set to use a Gateway with synsent
<a href="#">CSCVx64846</a>	"show sdwan policy service-path/tunnel-path" command cause device crash
<a href="#">CSCVx69830</a>	Cisco 1000 Series ASR: BQS crash seen at cpp_qm_event_proc_defer_cb
<a href="#">CSCVx72232</a>	rbuf-ooH crash in HSL
<a href="#">CSCVx73741</a>	custom app not getting detected after attached removed and re-attached- app-visibility is disabled
<a href="#">CSCVx75330</a>	fman_rp memory leak in acl_config_bind_v4_acl_message function.
<a href="#">CSCVx77203</a>	[17.5] Router crashed when sending traffic through non-SDWAN interface with DIA NAT + debug enabled
<a href="#">CSCVx78215</a>	An IOS XE device might crash at DoubleExceptionVector
<a href="#">CSCVx79113</a>	SDWAN cedge : traffic simulation tool shows traffic blackhole

Caveat ID Number	Description
<a href="#">CSCvx88246</a>	Packets dropped due to firewall + data policy interop issue
<a href="#">CSCvx89710</a>	SCEP: CA server fails to rollover CA certificate with error: "Storage not accessible"
<a href="#">CSCvx97718</a>	vtcp frees rx buffer when packet with expected next sequence arrives with no payload; phones reset
<a href="#">CSCvy30209</a>	IOS-XE cpp ucode crash with fragmented packets
<a href="#">CSCvy32673</a>	GD/1hx-Interface doesn't come up when reboot/upgrade device with autoneg enabled on 10G SFP+ Port

#### Open Bugs for Cisco IOS XE Amsterdam 17.3.4a

Caveat ID Number	Description
<a href="#">CSCvt62123</a>	DMVPN - after removing IPSec, traffic is dropped on a tunnel interface
<a href="#">CSCvu06483</a>	Data consistency errors seen on configuring mac-sec on the underlay interface with ipsec configured
<a href="#">CSCvv17346</a>	unexpected reload due to Crypto IKEv2 process
<a href="#">CSCvv38438</a>	Watchdog timeout due to Crypto IKMP
<a href="#">CSCvv48885</a>	can not update local-address in a crypto keyring
<a href="#">CSCvv82322</a>	Cisco 1001-X ASR and Cisco 9000 Series ASR: Link issue when using macsec
<a href="#">CSCvw48943</a>	crypto ikev2 proposals are not processed separately
<a href="#">CSCvw60359</a>	cEdge-policy: set next-hop-ipv6 is not working next-hop-ip (ipv4) is working.
<a href="#">CSCvw67366</a>	Cisco 1002-XASR: Punt keepalive crashed due to bqs related interrupt
<a href="#">CSCvw73769</a>	17.4 ZBFW:Cpp_cp crash seen when a rule is added at beginning in automation on Cisco 1000 Series ASR
<a href="#">CSCvw91361</a>	Crash when issuing "show crypto isakmp peers config"
<a href="#">CSCvw94166</a>	IKE should have a mechanism to alert or mitigate resource exhaustion due to QM flooding
<a href="#">CSCvx08118</a>	Cisco 1001-X ASR: Bug to further address CSCvt08179 : QFP crash due to hardware interrupt
<a href="#">CSCvx32807</a>	False positive alarm: IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL Fan Tray Bay 1 Fan Tray Module Missing
<a href="#">CSCvx41588</a>	Rapid memory exhaustion due to excessive logging
<a href="#">CSCvx74212</a>	IKEv1 IPSec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ

Caveat ID Number	Description
<a href="#">CSCvy10041</a>	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
<a href="#">CSCvy35853</a>	Cisco 1000 Series ASR- egress byte counter on MIP100 10GE interface is inaccurate
<a href="#">CSCvy54314</a>	Data-policy local-tloc with app-route is dropping packets when SLA is not met
<a href="#">CSCvy58115</a>	Cedge : Cloudexpress Office 365 probes are hitting 100% loss
<a href="#">CSCvy78123</a>	cEdge: High CPU usage due to Multicast and Data Policy configuration.
<a href="#">CSCvy82696</a>	cEdge dropping packets [combination /16, /17 data prefix with multiple ports in policy]
<a href="#">CSCvy91411</a>	AAR not correctly programmed in Cisco 1001-X ASR
<a href="#">CSCvy69555</a>	Unable to fetch eigrp prefix, nexthop, omptag, and route origin
<a href="#">CSCvu62879</a>	Crash@bgp_perform_general_scan

## Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.5

### Resolved Bugs for Cisco IOS XE Amsterdam 17.3.5

Caveat ID Number	Description
<a href="#">CSCvw84019</a>	show access-lists template summary not reflecting correct data
<a href="#">CSCvo41609</a>	GETVPN: Clearing members on Key Server causing rekey processing failure on GMs
<a href="#">CSCvz26211</a>	flow monitor statistics missing when reloading with configuration
<a href="#">CSCvy67657</a>	crypto ipsec security-association dummy leads to packet loss
<a href="#">CSCvy74799</a>	Ucode crash observed at tw_bad_timer_bucket () at ../../infra/tw_timer.c:918
<a href="#">CSCwa15132</a>	DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum
<a href="#">CSCvy85281</a>	Crash triggered by "crypto gdoi ks rekey replace-now"
<a href="#">CSCvy54606</a>	CVLA need to reserve at least 50M memory for low-end DRAM platform
<a href="#">CSCwa10915</a>	ASR1k PFRv3: Elephant flow will trigger performance monitor exporting more than 50% byte loss
<a href="#">CSCvy64468</a>	ASR1002-HX crashed after removing then applying the ZBF configuration.
<a href="#">CSCvx39529</a>	IKEv1/IKEv2 "show crypto session brief" output empty
<a href="#">CSCvy24571</a>	Static NAT conflicts/overwrites with Port-forwarding
<a href="#">CSCvx22349</a>	After reload or switchover, redundant ESP goes offline-&gt;online (transient issue)
<a href="#">CSCvy50292</a>	Standby router crashes ZBFW on VASI interfaces with FTP or SIP TCP traffic



Caveat ID Number	Description
<a href="#">CSCvy39195</a>	ESP200-X crash PA2_CSR32_TOP_CSR_PA_ERR_LEAF_INT__INT_PPE_INT1 with PPPoE/L2TP sessions
<a href="#">CSCvz86591</a>	VRF-aware static NAT with route-map and reversible not working
<a href="#">CSCvx32807</a>	False positive alarm: IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL Fan Tray Bay 1 Fan Tray Module Missing
<a href="#">CSCvy44951</a>	ESP Unexpected Reboot on Broadband Intelligent Services Gateway During Session Clean-up
<a href="#">CSCwa36699</a>	Prefetch CRL Download Fails
<a href="#">CSCvy35853</a>	ASR1k- egress byte counter on MIP100 10GE interface is inaccurate
<a href="#">CSCvz34290</a>	no ip nbar resources flow max-session does not restore default platform session limits
<a href="#">CSCvz73780</a>	memory leak with fman_cc process when SM-X-G4M2X module installed
<a href="#">CSCvy52359</a>	Segmentation fault(11), Process = CTS CORE - crash in ISR 4k
<a href="#">CSCvx41588</a>	Rapid memory exhaustion due to excessive logging
<a href="#">CSCvt66541</a>	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted
<a href="#">CSCvv38438</a>	Watchdog timeout due to Crypto IKMP
<a href="#">CSCvv17346</a>	unexpected reload due to Crypto IKEv2 process
<a href="#">CSCvz58895</a>	IOS-XE unable to export elliptic curve key
<a href="#">CSCvy89785</a>	OSPFv3 adjacency won't come up after "ospfv3 authentication ipsec" is applied on Tunnel interface
<a href="#">CSCvz03342</a>	Multicast boundary command on tunnel interface DMVPN network is sending ttl=1 packet
<a href="#">CSCvw91361</a>	Crash when issuing "show crypto isakmp peers config"
<a href="#">CSCvy69846</a>	Guestshell:.py files stored under /home/guestshell are lost after reboot on 1ng device
<a href="#">CSCvw48943</a>	crypto ikev2 proposals are not processed separately
<a href="#">CSCvz11362</a>	ASR fails to install rekey causing traffic drop

#### Open Bugs for Cisco IOS XE Amsterdam 17.3.5

Caveat ID Number	Description
<a href="#">CSCvy78087</a>	Qos download failed with FW policy when rebooting device
<a href="#">CSCvv81296</a>	Protocol specific change for base path

Caveat ID Number	Description
<a href="#">CSCvw81274</a>	Opflex generated Route Distinguisher is not globally unique on ASR1k
<a href="#">CSCvw70009</a>	ASR1K: fman_rp crash seen on 16.9.X when "show platform software nat RP active logging" is run
<a href="#">CSCvx94323</a>	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut
<a href="#">CSCwa49902</a>	MGCP automatic configuration fails after IOS-XE upgrade on ISR4k
<a href="#">CSCvx35902</a>	fman_rp: qos_hqf [L:1.0, N:0x3485061e18 ] (0p, 0c) download to FP failed resulting in a crash.
<a href="#">CSCwa58911</a>	Removing service-policy from the Zone-pair causes device crash
<a href="#">CSCvy10041</a>	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
<a href="#">CSCvv92630</a>	PKI http client fails to handle 1xx and 2xx responses
<a href="#">CSCvy79601</a>	ASR1001X gets rebooted when Tunnel move across two egress interfaces with QoS MPoL policy config
<a href="#">CSCwa39615</a>	Unexpected reload due to cpp-mcpl0-ucode failure
<a href="#">CSCwa17720</a>	Router rebooted de to watchdogs after issuing the commands sh crypto mib ipsec commands
<a href="#">CSCvw67366</a>	ASR1002-X: Punt keepalive crashed due to bqs related interrupt
<a href="#">CSCvz74322</a>	"Shutdown" command visible in running config after reload of ASR 1002-HX
<a href="#">CSCvz53819</a>	ZBFW : ARStandby drops seen on New Active during RG switchover
<a href="#">CSCwa34648</a>	Incorrect OMP Labels in On-Demand Tunnel H/S Topology
<a href="#">CSCvz54262</a>	ASR1001X crash at CFT after scaling up to 4M flows when internet link up from 2Gbps to 10Gbps
<a href="#">CSCvx64449</a>	%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: mac verify failed due to ip rtp header-compression iphc-format
<a href="#">CSCvw13048</a>	crash observed at NHRP while using summary-map
<a href="#">CSCvy57681</a>	Unexpected reboot of IOS-XE Router in BQS QM @ cpp_qm_proc_rt_commit
<a href="#">CSCvx74212</a>	IKEv1 IPsec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ
<a href="#">CSCwa51837</a>	Crash on cpp process when QoS policy configuration is being applied
<a href="#">CSCvv82322</a>	ASR1001-X and ASR9K: Link issue when using macsec
<a href="#">CSCwa18588</a>	IOSd Nhrp core due to a segmentation fault when disabling Pfr IWANs

Caveat ID Number	Description
<a href="#">CSCvz87460</a>	ASR 1000-RP2 VID>V07 16.9.7 MD5 signature does not match failure while upgrading to 17.3(1r) rommon
<a href="#">CSCvt62123</a>	DMVPN - after removing IPSec, traffic is dropped on a tunnel interface
<a href="#">CSCwa51443</a>	Incorrect check of the TCP sequence number causing return ICMP error packets to drop (Thousandeyes)
<a href="#">CSCvz28950</a>	DMVPN phase 2 connectivity issue between two spokes
<a href="#">CSCvy54048</a>	CPP Unexpected Reboot While Freeing CVLA Chunk
<a href="#">CSCvz62601</a>	ASR1000-MIP100 / IOS XE 17.3.2 / high CPU on LC process mcpecc-lc-ms and link flaps
<a href="#">CSCwa58533</a>	C1100 Unexpected reboot with Critical process fman_fp_image fault on fp_0_0
<a href="#">CSCvu77711</a>	Missing Mandatory Transform Type (ESN) in IKEv2 ESP Protocol
<a href="#">CSCwa30988</a>	CoS preservation not working for the services EVPL and EPL tunnel
<a href="#">CSCvy30606</a>	Device: sdn-network-infra-iwan key does not update successfully under network disruption situation
<a href="#">CSCvz65545</a>	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535
<a href="#">CSCvv55742</a>	GETVPN-ipv6 & LISP support on C900 platforms
<a href="#">CSCwa29964</a>	SCEP fails if AAAA DNS reply is received and source interface has no IPv6 address
<a href="#">CSCwa52627</a>	ASR1K / 17.3 / "sh int transceiver" reports incorrect Tx/Rx optical power values
<a href="#">CSCwa57462</a>	The router reload unexpectedly due to Cellular CNM process.
<a href="#">CSCwa61238</a>	FlexVPN per-user inline ACL from Radius not installed
<a href="#">CSCvx28426</a>	Router may crash due to Crypto IKMP process
<a href="#">CSCvy37152</a>	%CRIMSON-3-DATABASE_MEMLEAK: Database memory leak detected
<a href="#">CSCwa37243</a>	TenGigabitEthernet0/0/0-1 port keeps up/up status even the peer connecting port had been link down

## Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.6

### Resolved Bugs for Cisco IOS XE Amsterdam 17.3.6

Bug ID	Description
<a href="#">CSCwb46649</a>	NAT translation don't show (or use) correct timeout value for an established TCP session.
<a href="#">CSCvy78087</a>	Qos download failed with FW policy when rebooting device.

Bug ID	Description
<a href="#">CSCvz91309</a>	Crash due to IOSXE-WATCHDOG due to management port traffic storm.
<a href="#">CSCwa95092</a>	When object-group used in a ACL is updated, it takes no effect.
<a href="#">CSCwc36274</a>	CPP crash with performance monitor.
<a href="#">CSCwc19758</a>	CRC counter doesn't increase in "show interfaces" on device with EPA/MIP.
<a href="#">CSCvz87460</a>	MD5 signature does not match failure while upgrading to 17.3(1r) rommon.
<a href="#">CSCvy52143</a>	ENH: Address the memory fragmentation in "IPSEC Key" process.
<a href="#">CSCwc37320</a>	RP switchover causes linecard NFS mount failure resulting in memory leak.
<a href="#">CSCwa47219</a>	Crash on ipv4_nat_get_all_mapping_stats due to NULL pointer of mapping_hash_table.
<a href="#">CSCvz81956</a>	CHASSIS_MONITOR_ONLINE_TIME_EXCEEDED: R0/0: cmand: Reloading F0 because it has failed to come online.
<a href="#">CSCwc43794</a>	Device VRF+NAT Outside Source Static - Drop packets during FTP (Active-mode) execution.
<a href="#">CSCwc20005</a>	[XE ETA] IDP record is incomplete when traffic is fragmented.
<a href="#">CSCwa25614</a>	%SCHED-3-SEMLOCKED: SIP0/1: Exec attempted to lock a semaphore, already locked by itself.
<a href="#">CSCvz62601</a>	High CPU on LC process mcpcclc-ms and link flaps.
<a href="#">CSCvy37152</a>	Oper database memory leak detected.
<a href="#">CSCwc10160</a>	Device with EPA interface - "giants" counter keeps increasing after initial reception of giant.
<a href="#">CSCvz95158</a>	IPSec LED doesn't lit even though module is correctly installed.
<a href="#">CSCwb23043</a>	MACSEC not working on subinterfaces using dot1q &gt;255.
<a href="#">CSCwc06967</a>	IOS PKI client uses incorrect search filter for CRL retrieval using LDAPv3.
<a href="#">CSCvz92994</a>	Lack of MAC address in inform event message.
<a href="#">CSCwcl3013</a>	IPSec Key engine process holding memory continuously and not freeing up.
<a href="#">CSCwa17720</a>	Router rebooted due to watchdogs after issuing the commands SH Crypto MIB IPSec commands.
<a href="#">CSCwb65455</a>	Renewing hardware wan edge cert shows old cert serial/valid date in control local-properties.
<a href="#">CSCwb85046</a>	Device reloads when group-range is configured under an interface Group-Async.
<a href="#">CSCwb91026</a>	Traffic is hitting wrong sequence in the data policy.
<a href="#">CSCwa66916</a>	VG450 - SCCP auto-configuration issues with multiple protocols.

Bug ID	Description
<a href="#">CSCwb25913</a>	(Rework): After configuring match input-interface on class-map, router goes into a reboot loop.
<a href="#">CSCwb04815</a>	NHRP process taking more CPU with IP NHRP redirect configured.
<a href="#">CSCwa72273</a>	ZBFW dropping return packets from Zscaler tunnel post cedge upgrade.
<a href="#">CSCwb25137</a>	[XE NAT] Source address translation for multicast traffic fails with route-map.
<a href="#">CSCvy69405</a>	Appnav-XE connections are going as passthrough unsupported.
<a href="#">CSCwb55683</a>	Large number of IPSec tunnel flapping occurs when underlay is restored.
<a href="#">CSCwa80826</a>	Platforms running 17.x - crypto ipsec policy installation fails.
<a href="#">CSCwa67398</a>	NAT translations do not work for FTP traffic.
<a href="#">CSCwa51443</a>	Incorrect check of the TCP sequence number causing return ICMP error packets to drop (Thousandeyes).
<a href="#">CSCwb24123</a>	Registration of spoke fails with dissimilar capabilities w.r.t to HUB.
<a href="#">CSCvw16093</a>	Secure key agent trace levels set to Noise by default.
<a href="#">CSCwa84919</a>	"Revocation-check crl none" does not failover to NONE DNAC-CA.
<a href="#">CSCwb14020</a>	Serial interface stuck in "line protocol is down" state after it went down and it is recovered.
<a href="#">CSCvu70609</a>	Observed crash in device with prd10 image.
<a href="#">CSCwb15331</a>	Keyman memory leak using public keys.
<a href="#">CSCvy30606</a>	Device fails to update sdn-network-infra-iwan key after 1 year.
<a href="#">CSCwb76988</a>	IKEv2 fragmentation causes wrong message ID used for EAP authentication.
<a href="#">CSCwb99793</a>	CRL verification failure result 400 Bad Request with DigiCert.
<a href="#">CSCvz34668</a>	Static mapping for the hub lost on one of the spokes.
<a href="#">CSCwb95559</a>	Packet sanity failed for resolution reply on spoke due to missing SMEF capability.
<a href="#">CSCwa68540</a>	FTP data traffic broken when UTD IPS enabled in both service VPN.

#### Open Bugs for Cisco IOS XE Amsterdam 17.3.6

Caveat ID Number	Description
<a href="#">CSCvz65764</a>	Peer MSS value showing incorrect.
<a href="#">CSCwb53709</a>	PRP trailer frames were trunked in xconnect on Utah platform.

Caveat ID Number	Description
<a href="#">CSCvw81274</a>	Opflex generated Route Distinguisher is not globally unique on device.
<a href="#">CSCvw70009</a>	Device crash seen when "show platform software nat RP active logging" is run.
<a href="#">CSCwc18977</a>	Crash with "IPE_CPE_U14_CSR32_IPE_CPE_ERR_CPE_MISC_LEAF_INT__INT_CPE_MALGN_ADDR_ERR" error.
<a href="#">CSCwc03478</a>	VTCP does not support L2 correctly.
<a href="#">CSCvx35902</a>	fman_rp: qos_hqf [L:1.0, N:0x3485061e18 ] (0p, 0c) download to FP failed resulting in a crash.
<a href="#">CSCwb61073</a>	BQS Failure - Qos policy is missing in hardware for some Virtual-Access tunnels after session flaps.
<a href="#">CSCvu06483</a>	Data consistency errors seen on configuring mac-sec on the underlay interface with ipsec configured.
<a href="#">CSCvw67366</a>	Punt keepalive crashed due to bqs related interrupt.
<a href="#">CSCwb55514</a>	Crash seen after enabling "platform qos port-channel-aggregate".
<a href="#">CSCvz74322</a>	"Shutdown" command visible in running config after reload of device.
<a href="#">CSCwc59598</a>	Device statistics collection causing service-side BFD to flap on every collection interval.
<a href="#">CSCvw13048</a>	Crash observed at NHRP while using summary-map.
<a href="#">CSCwb76976</a>	NETFLOW SIP destination/source field contains garbage value.
<a href="#">CSCwa30988</a>	CoS preservation not working for the services EVPL and EPL tunnel.
<a href="#">CSCwc26669</a>	TLB miss for lock address during FNF cache lookup.
<a href="#">CSCwa97171</a>	PRP frames not transparent transmitted over L2TPv3 or EoMPLS tunnel.
<a href="#">CSCwb03893</a>	When MACSEC dot1q-in-clear 1 is enabled on interfaces there is traffic drop.
<a href="#">CSCwb51238</a>	Router reload unexpectedly two times when enter NETFLOW show command.
<a href="#">CSCvz59621</a>	MKA Session not coming up on EVC.
<a href="#">CSCwa98617</a>	Memory leak in AEM chunks related to firewall.
<a href="#">CSCwc20286</a>	Oceon processor hang followed by ESP100 crash.
<a href="#">CSCwb73395</a>	Need CLI option to disable ALG.
<a href="#">CSCvz28950</a>	DMVPN phase 2 connectivity issue between two spokes.
<a href="#">CSCvy90763</a>	PYON: Adjusting new text segment to address L2i rejections issues with SDWAN profiles.

Caveat ID Number	Description
<a href="#">CSCvz65545</a>	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535.
<a href="#">CSCwa52627</a>	Incorrect Tx/Rx optical power values reported for QSFP transceivers.
<a href="#">CSCwc20171</a>	Fragmented packets crashes while allocating memory.
<a href="#">CSCvx00230</a>	Device may show input/output rate values even if the interface is in admin down state.
<a href="#">CSCwb72336</a>	ICMP traceroute return packet not classified based on FW override port info.
<a href="#">CSCwa76570</a>	ISG / Crashes due to %IDMGR-3-INVALID_ID: bad id in id_delete during session roaming.
<a href="#">CSCvx94323</a>	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut.
<a href="#">CSCwa43562</a>	Device link goes err-disabled due to link-flap after reloading Catalyst 8300 peer device.
<a href="#">CSCwb66749</a>	When configuration ip nat inside/outside on VASI interface,ack/seq number abnormal.
<a href="#">CSCvy10041</a>	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map.
<a href="#">CSCwa13553</a>	Device QFP core due to NAT scaling issue.
<a href="#">CSCvy79601</a>	Device gets rebooted when Tunnel move across two egress interfaces with QoS MPoL policy config.
<a href="#">CSCwa69101</a>	ISG: initiator unclassified ip-address LQIPv4 command has no effect.
<a href="#">CSCvz53819</a>	ZBFW : AR Standby drops seen on New Active during RG switchover.
<a href="#">CSCvz63684</a>	EWC HA pair experiencing IOS tracebacks, followed by KEYMAN crash.
<a href="#">CSCwc22314</a>	RTSP Traffic not being rewritten by NAT.
<a href="#">CSCwb17282</a>	Router crashing when clearing a VPDN session.
<a href="#">CSCvx74212</a>	IKEv1 IPsec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ.
<a href="#">CSCwb08057</a>	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
<a href="#">CSCwc25291</a>	[Verizon CAP]NIM-LTE-EA No data - requires subslot reload to recover.
<a href="#">CSCwb14888</a>	Unable to remove "switchport mode access" and "switchport nonegotiate" at the same time.
<a href="#">CSCwb12647</a>	Device crash for stuck threads in cpp on packet processing.
<a href="#">CSCwc39865</a>	Subscriber session getting stuck and needs clearing it manually.
<a href="#">CSCwa57462</a>	The router reload unexpectedly due to Cellular CNM process.
<a href="#">CSCvt62123</a>	DMVPN - after removing IPsec, traffic is dropped on a tunnel interface.

Caveat ID Number	Description
<a href="#">CSCwb41907</a>	CPP uCode crash due to IPC congestion from DP to CP.
<a href="#">CSCwb46968</a>	Device template attachment causes pppoe commands to be removed from ethernet interface.
<a href="#">CSCvy54048</a>	CPP unexpected reboot while freeing CVLA chunk.
<a href="#">CSCwa76260</a>	IKEv2 deprecated ciphers denied by crypto engine CDSL - PSB security compliance - DES, 3DES, DH1/2/5.
<a href="#">CSCvu77711</a>	Missing mandatory transform type (ESN) in IKEv2 ESP Protocol.
<a href="#">CSCwa76875</a>	After configuring match input-interface on class-map, router goes into a reboot loop.
<a href="#">CSCvv55742</a>	GETVPN-ipv6 & LISP support on device platforms.
<a href="#">CSCwc30050</a>	UTD: Exception in utd_logger.py due to missing extra-data in AMP alert.
<a href="#">CSCwb02142</a>	Traceback: fman_fp_image core after clearing packet-trace conditions.
<a href="#">CSCvx73750</a>	Hightower 5G light is blue when 4G LTE is in use.
<a href="#">CSCvx28426</a>	Router may crash due to Crypto IKMP process.

## Resolved and Open Bugs for Cisco IOS XE Amsterdam 17.3.7

### Resolved Bugs for Cisco IOS XE Amsterdam 17.3.7

Bug ID	Description
<a href="#">CSCwd06372</a>	Unconditional excessive logging in EoGRE tunnel error handling case.
<a href="#">CSCwc26669</a>	TLB miss for lock address during FNF cache lookup.
<a href="#">CSCwd25107</a>	Interface VLAN 1 placed in shutdown state when configured with <b>ip address pool</b> .
<a href="#">CSCwc84967</a>	Intermittent double DTMF due to changing timestamp on a DTMF event.
<a href="#">CSCwd30578</a>	Wired guest client stuck at IP_LEARN with DHCP packets not forwarded out of the foreign to anchor.
<a href="#">CSCwc82140</a>	QFP crash when ZBFW configuration features <b>log dropped-packets</b> configuration.
<a href="#">CSCwa57462</a>	The router reload unexpectedly due to Cellular CNM process.
<a href="#">CSCwb41907</a>	ezPM(performance monitor) error logs may cause uCode crash due to congestion of IPC from DP to CP.
<a href="#">CSCwd81357</a>	QoS Classification not working for DSCP or ACL + MPLS EXP.
<a href="#">CSCwc72923</a>	ERROR info: Router configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt.
<a href="#">CSCwc70511</a>	Router reloads unexpectedly during NHRP processing.



Bug ID	Description
<a href="#">CSCwd76176</a>	DSPware 55.1.6 Release targeting v173_throttle.

#### Open Bugs for Cisco IOS XE Amsterdam 17.3.7

Bug ID	Description
<a href="#">CSCvz89354</a>	Router crashes due to CPUHOG when walking Cisco Flash MIB.
<a href="#">CSCvz73202</a>	TCAM parity error - QFP crash with a scale configuration.
<a href="#">CSCwa69101</a>	ISG: initiator unclassified IP-address LQIPv4 command has no effect.
<a href="#">CSCwa76875</a>	After configuring <b>match input-interface</b> on class-map, router goes into a reboot loop.
<a href="#">CSCvx77024</a>	IPv6 DMVPN - NBMA address not getting preserved.
<a href="#">CSCwe12194</a>	Auto-update cycle incorrectly deletes certificates.
<a href="#">CSCvy38743</a>	CISCO-CLASS-BASED-QOS-MIB doesn't work with LTE Cellular interface on device after reload.
<a href="#">CSCwa76570</a>	ISG/Crashes due to %IDMGR-3-INVALID_ID: bad id in id_delete during session roaming.
<a href="#">CSCwc39865</a>	Subscriber session getting stuck and needs clearing it manually.
<a href="#">CSCwa98617</a>	Memory Leak in AEM chunks related to Firewall.
<a href="#">CSCvz63684</a>	EWC HA pair experiencing IOS Tracebacks, followed by KEYMAN crash.
<a href="#">CSCwb02142</a>	Traceback: fman_fp_image core after clearing packet-trace conditions.
<a href="#">CSCwa43562</a>	Device link goes err-disabled due to link-flap after reloading peer device.
<a href="#">CSCwb61073</a>	BQS Failure - Qos policy is missing in hardware for some Virtual-Access tunnels after session flaps
<a href="#">CSCwa67851</a>	Router traceback and reload when different encapsulation used on xconnect interfaces.
<a href="#">CSCwb46968</a>	Device template attachment causes PPPoE commands to be removed from ethernet interface.
<a href="#">CSCwc76044</a>	Interface stats are not getting updated for port-channel.
<a href="#">CSCvx35902</a>	fman_rp: qos_hqf [L:1.0, N:0x3485061e18 ] (0p, 0c) download to FP failed resulting in a crash.
<a href="#">CSCwd84599</a>	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
<a href="#">CSCwd59722</a>	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
<a href="#">CSCwb78173</a>	CSDL failure: IPSec QM use of DES by Encrypt Proc is denied.
<a href="#">CSCwe41234</a>	VG450 VMWI race condition causes no ringing for analog phones.

## ROMmon Release Requirements

For more information on ROMmon support for Route Processors (RPs), Embedded Services Processors (ESPs), Modular Interface Processors (MIPs), and Shared Port Adapter Interface Processors (SIPs) on Cisco ASR 1000 Series Aggregation Services Routers, see <https://www.cisco.com/c/en/us/td/docs/routers/asr1000/rommon/asr1000-rommon-upg-guide.html>



---

**Note** After upgrading the ROMmon to version 17.3(1r), you cannot revert it to a version earlier than 17.3(1r) for the following platforms:

- ASR 1001-X
- ASR 1001-HX
- ASR 1002-HX
- ASR 1000-RP3

This restriction is only applicable for these platforms. If you have upgraded to ROMmon version 17.3(1r) on any other platform, reverting to an earlier version of ROMmon is permitted and does not cause any technical issues.

---

## Related Documentation

- [Release Notes for Previous Versions of ASR 1000 Series Aggregation Services Routers](#)
- [Hardware Guides for Cisco ASR 1000 Series Aggregation Services Routers](#)
- [Configuration Guides for ASR 1000 Series Aggregation Services Routers](#)
- [Command Reference Guides for ASR 1000 Series Aggregation Services Routers](#)
- [Product Landing Page for ASR 1000 Series Aggregation Services Routers](#)
- [Datasheet for ASR 1000 Series Aggregation Services Routers](#)
- [Upgrading Field Programmable Hardware Devices for Cisco ASR 1000 Series Routers](#)
- [Cisco ASR 1000 Series Aggregation Services Routers ROMmon Upgrade Guide](#)
- [Field Notices](#)
- [Deferral Notices](#)
- [Cisco Bulletins](#)

