



# Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE Amsterdam 17.3.x

---

**First Published:** 2020-07-31

**Last Modified:** 2023-10-28

## Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

## About Cisco 1000 Series Integrated Services Routers

The Cisco 1000 Series Integrated Services Routers (also referred to as router in this document) are powerful fixed branch routers based on the Cisco IOS XE operating system. They are multi-core routers with separate core for data plane and control plane. There are two primary models with 8 LAN ports and 4 LAN ports. Features such as Smart Licensing, VDSL2 and ADSL2/2+, 802.11ac with Wave 2, 4G LTE-Advanced and 3G/4G LTE and LTEA Omnidirectional Dipole Antenna (LTE-ANTM-SMA-D) are supported on the router.



---

**Note** Starting with Cisco IOS XE Amsterdam 17.3.2 release, 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-Hardware and Software Features

### New and Changed Hardware Features

#### New Hardware Features

There are no new hardware features in the Cisco IOS XE Amsterdam 17.3.1 release.

### New and Changed Software Features in Cisco IOS XE 17.3.8a

There are no new features in this release. This release provides a fix for [CSCwh87343](#): Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see the Security Advisory: [cisco-sa-iosxe-webui-privesc-j22SaA4z](#).

### New and Changed Software Features in Cisco IOS XE 17.3.8

There are no new software features in this release.

### New and Changed Software Features in Cisco IOS XE 17.3.7

There are no new software features in this release.

### New and Changed Software Features in Cisco IOS XE 17.3.6

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.3.5

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.3.4

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.3.3

**Table 1: New Software Features in Cisco ISR1000 Series Release, Cisco IOS XE Bengaluru 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.</p> <p>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>

## New and Changed Software Features in Cisco IOS XE 17.3.2



**Note** Starting with Cisco IOS XE Amsterdam 17.3.2, 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).

Table 2: New Software Features in Cisco ISR1000 Series Release, Cisco IOS XE Bengaluru 17.3.2

Feature	Description
<a href="#">Smart Licensing Using Policy</a>	<p>An enhanced version of Smart Licensing with the overall objective of providing a licensing solution that does not interrupt the operations of your network but also 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. 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 which 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>Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to the current version of the release.</p> <p>By default, your Smart Account and Virtual Account in CSSM are enabled for Smart Licensing Using Policy.</p> <p>For conceptual, configuration, migration, and troubleshooting information for Smart Licensing Using Policy, see the <a href="#">Smart Licensing Using Policy for Cisco Enterprise Routing Platforms</a> Guide.</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>
<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 Changed Software Features in Cisco IOS XE 17.3.1

Table 3: New Software Features in Cisco ISR1000 Series Release, Cisco IOS XE Bengaluru 17.3.1

Feature	Description
<a href="#">Dial Peer Binding with Live Traffic</a>	With the Live Bind feature, you can 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="#">Posture Assessment Support</a>	This feature enables you to utilize Posture Assessment capabilities to validate the compliance of endpoints according to security policies of your enterprise. Identity Services Engine (ISE) Posture functions are integrated into Cisco 1100 Integrated Services Routers. This feature can only be configured using the Add-On feature template in Cisco vManage.
<b>show ip nat pool</b>	The output of the <b>show ip nat pool</b> command provides extra details from this release.
<b>show ip cef <i>prefix</i> all</b>	To display all information of CEF, run the <b>show ip cef</b> command. This command in turn displays the output of other show commands therefore avoiding the need to run each of these commands individually: <ul style="list-style-type: none"> <li>- show ip route &lt;network&gt; &lt;network mask&gt;</li> <li>- show ip cef &lt;network&gt; &lt;network mask&gt; internal</li> <li>- show adjacency &lt;adj_id&gt; internal</li> <li>- show platform software ip rp active cef prefix &lt;network&gt;/&lt;mask_length&gt; detail</li> <li>- show platform software adjacency rp active index &lt;platform_adj_id&gt;</li> <li>- show platform software ip fp active cef prefix &lt;network&gt;/&lt;mask_length&gt; detail</li> <li>- show platform software adjacency fp active index &lt;platform_adj_id&gt;</li> <li>- show platform hardware qfp active feature cef-mpls adjacency handle &lt;cpp_handle_id&gt;</li> </ul>
<a href="#">IPv6 Virtual-PPP interface</a>	IPv6 and dual-stack is supported over Virtual-PPP and L2TPv2. This feature enhancement gives the capability of dual-stack support (flow of both IPv4 and IPv6 packets) over Virtual-PPP and L2TPv2.
<a href="#">TLS Server Name Indication (SNI) - RFC6066</a>	With this feature, 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.
<a href="#">Up to 100 VRF Instances</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 that need to support greater number of tenants per box, the limit of VRF instances is enhanced to 100 with this feature. Also, support is introduced for this feature in CUBE Enterprise with this release.
<a href="#">Media Proxy Multi-forking using SIPREC</a>	With this feature, the SIPREC-based CUBE Media Proxy solution now supports forking to multiple recorders.
<a href="#">OPUS Codec Negotiation</a>	With this feature, support is introduced for OPUS audio codec with CUBE.

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 being 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.



**Note** All pyang models are not fully compliant with all the IETF guidelines. For some pyang models, the errors and warnings display while executing pyang with .lintflag; these are 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 toolchains. To determine the issues with the pyang models, ensure to enable the pyang.lintflag and then run the check-models.sh script.

It is recommended to ignore *LEAFREF\_IDENTIFIER\_NOT\_FOUND* and *STRICT\_XPATH\_FUNCTIONS* errors.

## Cisco ISR1000 ROMMON Compatibility Matrix

The following table lists the ROMmon releases supported in Cisco IOS XE 16.x.x releases and Cisco IOS XE 17.x.x releases

**Table 4: Minimum and Recommended ROMmon Releases Supported on Cisco 1000 Series Integrated Services Routers**

Cisco IOS XE Release	Minimum ROMmon Release Supported for IOS XE	Recommended ROMmon Release Supported for IOS XE
16.6.x	16.6(1r)	16.6(1r)
16.7.x	16.6(1r)	16.6(1r)
16.8.x	16.8(1r)	16.8(1r)
16.9.x	16.9(1r)	16.9(1r)
16.10.x	16.9(1r)	16.9(1r)
16.11.x	16.9(1r)	16.9(1r)
16.12.x	16.9(1r)	16.12(1r)
17.2.x	16.9(1r)	16.12(1r)
17.3.x	16.9(1r)	16.12(1r)

## Resolved and Open Caveats

### About the Cisco Bug Search Tool

Use the [Cisco Bug Search Tool](#) to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

### Resolved Caveats in Cisco IOS XE Amsterdam 17.3.8a

All resolved bugs for this release are available in the [Cisco Bug Search Tool](#).

Bug ID	Description
<a href="#">CSCwh87343</a>	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: <a href="#">cisco-sa-iosxe-webui-privesc-j22SaA4z</a>

### Open Caveats in Cisco IOS XE Amsterdam 17.3.8a

Caveat ID Number	Description
<a href="#">CSCwa69101</a>	Initiator unclassified IP address LQipv4 command has no effect.
<a href="#">CSCwa76875</a>	After configuring match input-interface on class-map, router goes into a reboot loop.
<a href="#">CSCwb18108</a>	Unable to boot due to TAM Status TAM_LIB_ERR_WRITE_FAILURE.
<a href="#">CSCwe60059</a>	Crash when using dial-peer groups with STCAPP.
<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="#">CSCvz89354</a>	Router running crashes due to CPUHOG when walking ciscoFlashMIB.
<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="#">CSCwd03931</a>	Crashes due to cpp_cp_svr fault on fp_0_0 (rc=134) when applying umbrella dnsencrypt to profile.

Caveat ID Number	Description
<a href="#">CSCwb03455</a>	Inter-vrf route leaking not working and packet drop seen due to IPv4 unclassified.
<a href="#">CSCwf03193</a>	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine.
<a href="#">CSCwa43562</a>	Link goes err-disabled due to link-flap after reloading peer device.
<a href="#">CSCwf80400</a>	IOS XE router may experience unexpected reset while executing <b>show utd engine standard statistics</b> .
<a href="#">CSCwe12194</a>	Auto-update cycle incorrectly deletes certificates.
<a href="#">CSCwb46968</a>	Device template attachment causes PPPoE commands to be removed from ethernet interface.
<a href="#">CSCwe39011</a>	GARP on port up/up status from router is not received by remote peer device.
<a href="#">CSCvy54048</a>	CPP unexpected reboot while freeing CVLA chunk.
<a href="#">CSCwh26218</a>	Ce0/2/0 DDR: No free dialer - starting fast idle timer.
<a href="#">CSCwb78173</a>	CSDL failure: IPSec QM use of DES by encrypt proc is denied.
<a href="#">CSCwf48808</a>	FlexVPN: Stale client routes stuck in RIB on FlexServer.

### Resolved Caveats in Cisco IOS XE Amsterdam 17.3.8

There are no resolved caveats for the Cisco IOS XE Amsterdam 17.3.8 release.

### Open Caveats in Cisco IOS XE Amsterdam 17.3.8

Caveat ID Number	Description
<a href="#">CSCwa69101</a>	Initiator unclassified IP address LQipv4 command has no effect.
<a href="#">CSCwa76875</a>	After configuring match input-interface on class-map, router goes into a reboot loop.
<a href="#">CSCwb18108</a>	Unable to boot due to TAM Status TAM_LIB_ERR_WRITE_FAILURE.
<a href="#">CSCwe60059</a>	Crash when using dial-peer groups with STCAPP.
<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="#">CSCvz89354</a>	Router running crashes due to CPUHOG when walking ciscoFlashMIB.
<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.

Caveat ID Number	Description
<a href="#">CSCwd03931</a>	Crashes due to cpp_cp_svr fault on fp_0_0 (rc=134) when applying umbrella dnsencrypt to profile.
<a href="#">CSCwb03455</a>	Inter-vrf route leaking not working and packet drop seen due to IPv4 unclassified.
<a href="#">CSCwf03193</a>	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine.
<a href="#">CSCwa43562</a>	Link goes err-disabled due to link-flap after reloading peer device.
<a href="#">CSCwf80400</a>	IOS XE router may experience unexpected reset while executing <b>show utd engine standard statistics</b> .
<a href="#">CSCwe12194</a>	Auto-update cycle incorrectly deletes certificates.
<a href="#">CSCwb46968</a>	Device template attachment causes PPPoE commands to be removed from ethernet interface.
<a href="#">CSCwe39011</a>	GARP on port up/up status from router is not received by remote peer device.
<a href="#">CSCvy54048</a>	CPP unexpected reboot while freeing CVLA chunk.
<a href="#">CSCwh26218</a>	Ce0/2/0 DDR: No free dialer - starting fast idle timer.
<a href="#">CSCwb78173</a>	CSDL failure: IPsec QM use of DES by encrypt proc is denied.
<a href="#">CSCwf48808</a>	FlexVPN: Stale client routes stuck in RIB on FlexServer.

### Resolved Caveats in Cisco IOS XE Amsterdam 17.3.7

Caveat ID Number	Description
<a href="#">CSCwd30578</a>	Wired guest client stuck at IP_LEARN with DHCP packets not forwarded out of the foreign to anchor.

### Open Caveats in Cisco IOS XE Amsterdam 17.3.7

Caveat ID Number	Description
<a href="#">CSCwa98617</a>	Memory leak in AEM chunks related to firewall.
<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="#">CSCwd59722</a>	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
<a href="#">CSCwc76044</a>	Interface stats are not getting updated for port-channel

## Resolved Caveats in Cisco IOS XE Amsterdam 17.3.6

Caveat ID Number	Description
<a href="#">CSCwb23043</a>	MACSEC not working on subinterfaces using dot1q >255 between devices.
<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="#">CSCwc13013</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>	SCCP auto-configuration issues with multiple protocols.
<a href="#">CSCwb25913</a>	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 tunnel post device 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>	IOS-XE: Device platforms running - crypto ipsec policy installation fails.
<a href="#">CSCwa67398</a>	NAT translations do not work for FTP traffic in device.
<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="#">CSCvu70609</a>	Observed crash in device 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.

Caveat ID Number	Description
<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 Caveats in Cisco IOS XE Amsterdam 17.3.6

Caveat ID Number	Description
<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 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>	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 : ARStandby 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>	Device 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>	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.

Caveat ID Number	Description
<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.
<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="#">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="#">CSCvx28426</a>	Router may crash due to Crypto IKMP process.

### Resolved Caveats in Cisco IOS XE Amsterdam 17.3.5

Caveat ID Number	Description
<a href="#">CSCvy89785</a>	OSPFv3 adjacency won't come up after ospfv3 authentication ipsec is applied on Tunnel interface
<a href="#">CSCvz58895</a>	IOS-XE unable to export elliptic curve key
<a href="#">CSCvy87803</a>	Ethernet loopback not working
<a href="#">CSCvy20382</a>	Unexpected Reset in CMCC or CMAND on IOS-XE Router
<a href="#">CSCvw91361</a>	Crash when issuing show crypto isakmp peers config
<a href="#">CSCvy54606</a>	CVLA need to reserve at least 50M memory for low-end DRAM platform
<a href="#">CSCvy67657</a>	Crypto ipsec security-association dummy leads to packet loss
<a href="#">CSCvy24571</a>	Static NAT conflicts/overwrites with Port-forwarding
<a href="#">CSCvw48943</a>	Crypto ikev2 proposals are not processed separately
<a href="#">CSCvo41609</a>	GETVPN: Clearing members on Key Server causing rekey processing failure on GMs
<a href="#">CSCvy74799</a>	Ucode crash observed at tw_bad_timer_bucket () at ../.././infra/tw_timer.c:918

Caveat ID Number	Description
<a href="#">CSCwa15132</a>	DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum
<a href="#">CSCvy68270</a>	CWMP wrong parameter value
<a href="#">CSCvv38438</a>	Watchdog timeout due to Crypto IKMP
<a href="#">CSCwa36699</a>	Prefetch CRL Download Fails
<a href="#">CSCvx39529</a>	IKEv1/IKEv2 show crypto session brief output empty
<a href="#">CSCvt66541</a>	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted

### Open Caveats in Cisco IOS XE Amsterdam 17.3.5

Caveat ID Number	Description
<a href="#">CSCvv81296</a>	Protocol specific change for base path
<a href="#">CSCvx94323</a>	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut
<a href="#">CSCvw87352</a>	Missing Serial Number in DSLAM Inventory Check
<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="#">CSCvy79601</a>	Device gets rebooted when Tunnel move across two egress interfaces with QoS MPoL policy config
<a href="#">CSCwa17720</a>	Router rebooted de to watchdogs after issuing the commands sh crypto mib ipsec commands
<a href="#">CSCvy26572</a>	[SWI : #01080538 ] LTE is not reestablishing after reset of the modem
<a href="#">CSCwa50054</a>	Boot Levels Incorrectly Set when Legacy Traditional Licenses are Installed with Smart Licensing
<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="#">CSCwa49902</a>	MGCP automatic configuration fails after IOS-XE upgrade on ISR4k
<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="#">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

Caveat ID Number	Description
<a href="#">CSCwa18588</a>	IOSd Nhrp core due to a segmentation fault when disabling PfR IWANs
<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="#">CSCvy47279</a>	Device crashed when PPPoE(running NAT) cable pulled out
<a href="#">CSCwa58533</a>	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="#">CSCvy41947</a>	EIO: Packets getting reassembled and are forwarded as it is to the Gigabit interface
<a href="#">CSCvy30606</a>	Device: sdn-network-infra-iwan key does not update successfully under network disruption situation
<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="#">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

### Resolved Caveats in 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="#">CSCvw05211</a>	Pre-mature session deletion leading to churn and lower TPS at scale
<a href="#">CSCvw23197</a>	BFD sessions go down on Service VPN after UTD is enabled on cEdge
<a href="#">CSCvw81572</a>	Multiple crashes cpp_cp_svr and qfp-ucode on 16.12.4
<a href="#">CSCvw87300</a>	IP address not correctly in SIP traffic
<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="#">CSCvx29856</a>	Port mapping NAT configurations not saved to startup config

Caveat ID Number	Description
<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="#">CSCvx38454</a>	ISR Crash for CENT-MC-0 process
<a href="#">CSCvx45788</a>	cannot apply ciscosdwan.cfg due to vpg-log-server-acl ACL on VirtualPortGroup0 for logging
<a href="#">CSCvx49102</a>	PPPoE model enablement on CWMP
<a href="#">CSCvx53049</a>	Crash when TPOOL is updating and 'wr mem' is issues at same time
<a href="#">CSCvx55296</a>	CWMP: WANIPConnection.ExternalIPAddress sent in inform instead of WANPPPConnection.ExternalIPAddress
<a href="#">CSCvx55322</a>	CWMP configures PPP chap callin when username is configured
<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="#">CSCvx73741</a>	custom app not getting detected after attached removed and re-attached- app-visibility is disabled
<a href="#">CSCvx75352</a>	CWMP port mapping description is lost after CPE reload
<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
<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="#">CSCvy03589</a>	CWMP : Port mpping not created under WANPPP profile when WAN connection is set to PPP Dialer
<a href="#">CSCvy17964</a>	Traceback seen when cwmp wan default interface changed
<a href="#">CSCvy25957</a>	Security container is dropping legitimate FIN,ACK Packets

Caveat ID Number	Description
<a href="#">CSCvy30209</a>	IOS-XE cpp ucode crash with fragmented packets
<a href="#">CSCvy35044</a>	Signature update failure - SSL-CERTIFICATE_VERIFY_FAILED
<a href="#">CSCvy36311</a>	CWMP : Portmapping with space in description field rejected after reload
<a href="#">CSCvy39019</a>	CWMP: WANPPPConnection not reset when PPP credentials changed

### Open Caveats in 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="#">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="#">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="#">CSCvx74212</a>	IKEv1 IPSec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ
<a href="#">CSCvy10041</a>	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
<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="#">CSCvy67301</a>	URL Filtering regex pattern match not working on large pattern
<a href="#">CSCvy68270</a>	CWMP wrong parameter value
<a href="#">CSCvy73818</a>	cEdge QFP starts dropping traffic - UTD Service Node not healthy ident
<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="#">CSCvy69555</a>	Unable to fetch eigrp prefix, nexthop, omptag, and route origin

## Resolved Caveats in Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
<a href="#">CSCCuv97577</a>	Mishandling of dsmpSession pointer causes a crash
<a href="#">CSCCvu23516</a>	Static routes pointing to interface tunnel not valid after tunnel's source interface flaps.
<a href="#">CSCCvu32771</a>	IOSd Crash due to Segmentation fault at SISF Main Thread
<a href="#">CSCCvv03229</a>	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
<a href="#">CSCCvv09342</a>	Cloud Express probes fails when two default rules are present
<a href="#">CSCCvv40006</a>	Traceback: IP SLA triggers INJECT_HDR_LENGTH_ER and INJECT_FEATURE_ESCAPE log message
<a href="#">CSCCvv61770</a>	Crash seen in isis_sr_uloop_lspdb_dump with 'debug isis microloop' enabled
<a href="#">CSCCvv64633</a>	BGP: advertised community list is malformed due to GSHUT community
<a href="#">CSCCvv71775</a>	Cellular interface down/up frequently occurs with DoCoMo MVNO sim
<a href="#">CSCCvv78028</a>	No responder-bytes from cEdge when UTD is enabled
<a href="#">CSCCvv79273</a>	Router may crash when using Stateful NAT64
<a href="#">CSCCvv88621</a>	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage
<a href="#">CSCCvv91575</a>	Cisco 1111-8P ISR: NAT translations packet counter MIB OID counts unnecessary additional value
<a href="#">CSCCvv91865</a>	Moving PC from network causes static DHCP binding to be removed from the device.
<a href="#">CSCCvw06719</a>	"platform ipsec reassemble transit" tail-drops unencrypted IPv4 Fragments with specific payload
<a href="#">CSCCvw06780</a>	DMVPN with ipv6 link-local address do not register to HUB
<a href="#">CSCCvw09486</a>	Router might crash after apply a class-map in input direction with bandwidth percentage
<a href="#">CSCCvw10972</a>	NAT64 ALG: Router crashes on nat64_process_token
<a href="#">CSCCvw11902</a>	Passive FTP doesn't work with NAT
<a href="#">CSCCvw14131</a>	Crash in TCL Bytecode When Running RA Trace in Guestshell Python
<a href="#">CSCCvw14836</a>	ISR router running 16.9.6 crashes authenticating crypto certificate
<a href="#">CSCCvw16643</a>	Device Template failing to attach after changing few device variables
<a href="#">CSCCvw19171</a>	Smart license registration through explicit mode proxy server
<a href="#">CSCCvw19362</a>	[EVPN RT2-RT5] After few host moves RT2-RT5 re-origination happens even when there is no Remote RT2

Caveat ID Number	Description
<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>	ip-acl errors of correcting the logic of sequence id when there is an error with msg creation
<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="#">CSCvw36514</a>	cEdge crashes due to a large packet at vesen_ipsec_v4_input_get_vctrl_data
<a href="#">CSCvw36629</a>	cEdge: NATed tuple flips for HSL deleted flow
<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="#">CSCvw41482</a>	SSH with Certificate authentication doesn't work after upgrade to 17.3.1
<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="#">CSCvw48811</a>	RP went down due to __be_iosd_rec_malloc_free_before
<a href="#">CSCvw54076</a>	[SIT]: BFD sessions not established between Edges, with UTD enabled
<a href="#">CSCvw55030</a>	Dynamic Nat pool "ip aliases" are not created on the device
<a href="#">CSCvw56517</a>	LMR Unable to hear first seconds of audio
<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="#">CSCvw58646</a>	cEdge: Inspect rule cannot be modified to accept or drop without deactivating the policy
<a href="#">CSCvw62805</a>	SDWAN ZBFW CPU punted traffic mishandling -- Out2In packet looped
<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

Caveat ID Number	Description
<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="#">CSCvw97748</a>	Decouple mac aging from ARP aging on vlans not using the centralized gw feature
<a href="#">CSCvx02515</a>	BGP IPv6 link-local session doesn't come up
<a href="#">CSCvx08852</a>	Not able to create VFI instances
<a href="#">CSCvx12686</a>	Memory Lock and system crashed while clearing ip access-list stats.
<a href="#">CSCvx19135</a>	ISR crashes when ZBFW ALG inspects tunneled packet
<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 Caveats in Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
<a href="#">CSCvw88098</a>	cEdge crashes while running web traffic testing with security features enabled
<a href="#">CSCvw89001</a>	LTE interface is not getting IP address after upgrading the router.
<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="#">CSCvw96723</a>	CP process crashed while I95 driver was adding an IPC response to the receive ring
<a href="#">CSCvx02009</a>	cEdge running 17.3.2 crashed - Critical software exception / IOSXE-WATCHDOG: Process = SNMP ENGINE
<a href="#">CSCvx14095</a>	NETCONF ACL not working if ACL is referencing an object-group.
<a href="#">CSCvx18526</a>	Clients using DHCP Server Port-Based Address Allocation not getting IP address.
<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

Caveat ID Number	Description
<a href="#">CSCvx35902</a>	fman_rp: qos_hqf [L:1.0, N:0x3485061e18 ] (Op, Oc) download to FP failed resulting in a crash.
<a href="#">CSCvx38454</a>	ISR Crash for CENT-MC-0 process
<a href="#">CSCvx40030</a>	IP PIM SPT-threshold infinity causes ICMP Echo Replies to not be generated for IP Multicast Requests

### Resolved Caveats in Cisco IOS XE Amsterdam 17.3.2

Caveat ID Number	Description
<a href="#">CSCvv85766</a>	Memory leak upon ssh/scp connections to a router
<a href="#">CSCvj29514</a>	CME: Toll fraud app not automatically trusting traffic from phones
<a href="#">CSCvp73666</a>	DNA - LAN Automation doesn't configure link between Peer Device and PnP Agent due CDP limitation
<a href="#">CSCvq65366</a>	Cube might crash when sending a SIP message over TLS
<a href="#">CSCvq73575</a>	TCP traceroute - response ICMP TTL exceeded packet dropped by ZBFW with NAT enabled
<a href="#">CSCvq90343</a>	Secure SIP trunk between SIP-GW/CUBE and CUCM with multiple nodes not coming in to service.
<a href="#">CSCvq97906</a>	"DHCPD Receive" process crash
<a href="#">CSCvq98999</a>	Crash when IPSEC SA installation fails @ imgr_ipsec_sa_n2_install_done
<a href="#">CSCvq99498</a>	Crashes when trying to bring-up / bring-down IPsec crypto session for OSPFv3
<a href="#">CSCvr01327</a>	incorrect Total number of translations on show ip nat translations
<a href="#">CSCvr01454</a>	Punt fragment crash when receive EoGRE packets which have many fragments
<a href="#">CSCvr05213</a>	Smart licensing PID and SN logs filling up the IOSRP tracelogs
<a href="#">CSCvr05504</a>	Dialer interface counter does not correlate to the counter of interfaces bounded to
<a href="#">CSCvr12455</a>	KPML dialing fails after CSCvq20936 commit
<a href="#">CSCvr13358</a>	STUN packet breaks MOH RTP packet flow
<a href="#">CSCvr13385</a>	CUBE/LGW: STUN Indication packets generated constantly for call forking flows
<a href="#">CSCvr17169</a>	qfp ucode crash with media monitor
<a href="#">CSCvr24316</a>	Router crashes due to Segmentation Fault when 'ccb' gives a NULL Pointer
<a href="#">CSCvr26524</a>	Crash due to NBAR classification

Caveat ID Number	Description
<a href="#">CSCvr31188</a>	GETVPN gikev2 Secondary KS doesn't push new policy after merging split condition
<a href="#">CSCvr33415</a>	Router may crash unexpectedly with Segmentation fault(11), Process = DSMP
<a href="#">CSCvr39932</a>	IPSEC install failed IPSEC_PAL_SA shows "unexpected number of parents"
<a href="#">CSCvr41793</a>	IOS PKI: CRL retrieval does not use HTTP Content-Length
<a href="#">CSCvr48349</a>	ESP ucode crashed when running NAT with bpa (CGN)
<a href="#">CSCvr51860</a>	Observed Traceback with SRTP-RTP call after hold/resume
<a href="#">CSCvr57565</a>	MGCP Calls with SRTP fail to connect with Cause Value=47 due to T.38 calls
<a href="#">CSCvr58230</a>	While signalling forking the CUBE is not Sending Re-INVITE for T.38 with the Authorized header.
<a href="#">CSCvr80706</a>	IOSXE - ucode crash in ZBF during flow creation for TCP subflows
<a href="#">CSCvr90926</a>	CUBE is updating the resolved IP only after the REGISTER expires
<a href="#">CSCvr96597</a>	IOS-XE crash after doing a SCEP enrollment
<a href="#">CSCvs01943</a>	"login authentication VTY_authen" is missing on "line vty 0 4" only
<a href="#">CSCvs13960</a>	IWAN High CPU and Memory
<a href="#">CSCvs26625</a>	C1113/1112 does not train up in ADSL2+ mode when configured in "operating mode auto"
<a href="#">CSCvs29535</a>	IWAN crash related to DCA channel
<a href="#">CSCvs47682</a>	Router crashed when attempting to remove a nonexistent trustpoint from dspfarm profile
<a href="#">CSCvs56721</a>	spoke-to-spoke PLR packets should not change the interface PLR status
<a href="#">CSCvt20318</a>	BGP Neighbors Stuck on Device
<a href="#">CSCvt48480</a>	Flow monitor is removed from interface configuration on reload
<a href="#">CSCvt62112</a>	Physical policy cannot be clean up with QoS policy in suspended mode on PPPoE Dialer
<a href="#">CSCvt91720</a>	router see http wsma request as coming from 192.168.1.5
<a href="#">CSCvu09862</a>	Call Rerouting functionality not working on 16.6/16.12/17.1 IOS-XE trains.
<a href="#">CSCvu18001</a>	Segmentation fault observed in BGP -"UNIX-EXT-SIGNAL: Segmentation fault(11), Process = BGP Scanner"
<a href="#">CSCvu19733</a>	Evaluation of CVE-2020-11868 for IOS
<a href="#">CSCvu26741</a>	Punt-Keepalive crash with lsmpl_lo_drv and container app traffic.

Caveat ID Number	Description
<a href="#">CSCvu27953</a>	Crash due to a segmentation fault in the "IPsec background proc" process
<a href="#">CSCvu54786</a>	Crash on configuring a highest key identifier for OSPF authentication under an interface
<a href="#">CSCvu65369</a>	Link auto-negotiation fails between C1111-4P ES-4 switch module and Meraki MX100
<a href="#">CSCvu70286</a>	L2RIB thread crashed after removing global vrf definition for evpn
<a href="#">CSCvu98884</a>	Rapid BFD events on CSR running HA solution causes CSR to get stuck in a non-operational state
<a href="#">CSCvv01445</a>	Router Crashes when advertised-routes command executed for neighbours
<a href="#">CSCvv02486</a>	Random MPLS-TE tunnels with explicit-path stay down after egress interface is bounced.
<a href="#">CSCvv04236</a>	IOS-XE: IPv6 OSPF authentication ipsec - adjacency fails
<a href="#">CSCvv08341</a>	Netconf deleting wrong IKEv2 parameters
<a href="#">CSCvv11443</a>	Assertion Failed in MFIB causes Catalyst 9500 Switch to crash
<a href="#">CSCvv13193</a>	Memory leak 'Admin group' with some triggers in ISIS
<a href="#">CSCvv17560</a>	BMP BGP server can lead to CPUHOG and crashes
<a href="#">CSCvv20380</a>	Removing and Adding Bulk ACL leads to Tracebacks and Error-Objects
<a href="#">CSCvv24156</a>	FlexAlgo: ISIS crash when ISIS adjacency goes down
<a href="#">CSCvv25401</a>	EWLC crash after querying an mDNS record
<a href="#">CSCvv26042</a>	ios crash at l2rib_server_ios_obj_notification
<a href="#">CSCvv26538</a>	Crash due to a NULL pointer while bringing down PPPoE sessions.
<a href="#">CSCvv29239</a>	EFT[TUD]: WLC crashed @ mdns_io_event_callback_v6
<a href="#">CSCvv43279</a>	[EVPN RT2-RT5] Routing Loop due to CGW re-originating the Type 2 MAC+IP with MAC+IP VRF details
<a href="#">CSCvv43957</a>	Template push on ISR1k not working due to no authentication timer reauthenticateError
<a href="#">CSCvv59662</a>	cEdge may crash when template with big security policy pushed
<a href="#">CSCvv64319</a>	bgp crash in bgp_show_network_detail, bgp_imp_find_imported_path_topo
<a href="#">CSCvv70274</a>	[EVPN BGP] crash@bgp_ipv6_best_metric, bgp_evpn_best_metric,bgp_best_metric,bgp_show_network_detail
<a href="#">CSCvv72254</a>	EVPN incorrect duplicate v4/v6 default routes, crash eventually
<a href="#">CSCvv78226</a>	cEdge does not install route from type3 LSA into the RIB from area 0

Caveat ID Number	Description
<a href="#">CSCvv94834</a>	BGP crash during IOL testbed launch

### Open Caveats in Cisco IOS XE Amsterdam 17.3.2

Caveat ID Number	Description
<a href="#">CSCvu77745</a>	PMAN-3-PROCFAIL: Chassis 1 R0/0: pman: R0/0: The process keyman has failed (rc 139)
<a href="#">CSCvu89597</a>	RM crash at __be_address_cmp __be_avl_get_next while doing shut/no shut or BR
<a href="#">CSCvu89599</a>	BR crash at __be_strlen __be_fman_rtmap_create_route_map_msg
<a href="#">CSCvv40206</a>	Router may crash under ZBF configuration
<a href="#">CSCvv51001</a>	Crash during BGP VPN route import
<a href="#">CSCvv79273</a>	Router may crash when using Stateful NAT64
<a href="#">CSCvv91204</a>	SSS crashed the router at the moment of freeing AAA req
<a href="#">CSCvw05211</a>	Pre-mature session deletion leading to churn and lower TPS at scale
<a href="#">CSCvw09093</a>	route not getting installed, need to remove and reattach the template
<a href="#">CSCvw14836</a>	ISR router running 16.9.6 crashes authenticating crypto certificate
<a href="#">CSCvw16643</a>	Device Template failing to attach after changing few device variables
<a href="#">CSCvw22760</a>	MACSEC MKA stops forwarding data after every 3rd rekey

### Resolved Caveats in Cisco IOS XE Amsterdam 17.3.1

Caveat ID Number	Description
<a href="#">CSCvv54943</a>	ISR1100: Bridge Domain does not pass traffic through SVI after an upgrade to 16.12.x onwards.
<a href="#">CSCvp24405</a>	Router crashes after adding macsec reply-protection command on an interface
<a href="#">CSCvs45107</a>	AnyConnect fails to reconnect when original session expires
<a href="#">CSCvs56559</a>	show crypto pki server shows wrong expire certificate date
<a href="#">CSCvs63841</a>	SDWAN ISR1100: No SW Image listed when .bin image booted from flash / usb
<a href="#">CSCvs65950</a>	IOS PKI: P12 not generated on IOS Sub CA at rollover certificate generation
<a href="#">CSCvs81967</a>	ISR4K: %BOOT-3-BOOT_SRC: R0/0: No space on boot /dev/bootflash5 for packages, using bootflash!
<a href="#">CSCvs88686</a>	ISR4K / ASR / CBR8 crash in cpp_cp_svr due to watchdog timeout

Caveat ID Number	Description
<a href="#">CSCvs96540</a>	SDWAN device admin-tech has empty "show running config" in /tech/ios file
<a href="#">CSCvs99705</a>	PKI CLI - no warning that rsakeypair name starting from 0 (zero) is not working for cert regenerate
<a href="#">CSCvt03869</a>	Router reloads due to crypto pki crl request <trustpoint-name> during get a fresh copy of CRL
<a href="#">CSCvt05373</a>	SDWAN device and vmanage is not in sync when manual software reset is done
<a href="#">CSCvt21263</a>	Crash upon delete of virtual-access when virtual-template has "no tunnel protection ipsec initiate"
<a href="#">CSCvt21691</a>	VLAN1 is allowed on the trunk port even though it is not allowed in configurations of C111 interface
<a href="#">CSCvt31561</a>	TBAR is not disabled in GM when it is disabled in KS
<a href="#">CSCvt35947</a>	Duplicate ipv6 address while connecting to remote client
<a href="#">CSCvt40523</a>	GETVPN: KS 16.12.x - COOP switchover causes GMs to immediately use new TEK rekey
<a href="#">CSCvt52051</a>	IPsec tunnel is getting established for a backup NHS DMVPN hub
<a href="#">CSCvt52825</a>	Memory leak in SCCP TLS Client on unexpected deregister event
<a href="#">CSCvt65588</a>	FlexVPN IKEv2 Tunnel route removed after establishing new IKEv2 SA to another peer
<a href="#">CSCvu82189</a>	Enabling guestshell gives "float division by zero"

### Open Caveats in Cisco IOS XE Amsterdam 17.3.1

Caveat ID Number	Description
<a href="#">CSCvv02180</a>	C1113-8PLTEEAWA failed to boot: Package does not support : PID not supported in 17.4
<a href="#">CSCvu59956</a>	IOS cannot boot with 16.12(1r) or later rommon due to cookie PID field incorrectly programmed
<a href="#">CSCvu92277</a>	Memory leak observed for FTM process leading to a device crash eventually.

### Related Information

- [Hardware Installation Guide](#)
- [Software Configuration Guide](#)
- [Smart Licensing using Policy](#)

## Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

### Cisco Bug Search Tool

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

## Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

## Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at <https://www.cisco.com/en/US/support/index.html>.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.

