



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.

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 Smart Licensing Using Policy for Cisco Enterprise Routing Platforms.</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
Smart Licensing Using Policy	<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 Smart Licensing Using Policy for Cisco Enterprise Routing Platforms Guide.</p> <p>For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.</p>
Cisco DNA Support for Smart Licensing Using Policy	<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>Note On the Cisco DNA Center GUI, you can generate a SLAC only for HSECK9 licenses, and only for certain product instances. See the configuration guide 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
Dial Peer Binding with Live Traffic	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.
Posture Assessment Support	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.
show ip nat pool	The output of the show ip nat pool command provides extra details from this release.
show ip cef <i>prefix</i> all	To display all information of CEF, run the show ip cef 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"> - show ip route <network> <network mask> - show ip cef <network> <network mask> internal - show adjacency <adj_id> internal - show platform software ip rp active cef prefix <network>/<mask_length> detail - show platform software adjacency rp active index <platform_adj_id> - show platform software ip fp active cef prefix <network>/<mask_length> detail - show platform software adjacency fp active index <platform_adj_id> - show platform hardware qfp active feature cef-mpls adjacency handle <cpp_handle_id>
IPv6 Virtual-PPP interface	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.
TLS Server Name Indication (SNI) - RFC6066	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.
Up to 100 VRF Instances	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.
Media Proxy Multi-forking using SIPREC	With this feature, the SIPREC-based CUBE Media Proxy solution now supports forking to multiple recorders.
OPUS Codec Negotiation	With this feature, support is introduced for OPUS audio codec with CUBE.

Feature	Description
Consumption of INVITE with Replaces	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
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z

Open Caveats in Cisco IOS XE Amsterdam 17.3.8a

Caveat ID Number	Description
CSCwa69101	Initiator unclassified IP address LQipv4 command has no effect.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwb18108	Unable to boot due to TAM Status TAM_LIB_ERR_WRITE_FAILURE.
CSCwe60059	Crash when using dial-peer groups with STCAPP.
CSCwa76570	ISG/crashes due to %IDMGR-3-INVALID_ID: bad id in id_delete during session roaming.
CSCwc39865	Subscriber session getting stuck and needs clearing it manually.
CSCvz89354	Router running crashes due to CPUHOG when walking ciscoFlashMIB.
CSCvz63684	EWC HA pair experiencing IOS tracebacks, followed by KEYMAN crash.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCwd03931	Crashes due to cpp_cp_svr fault on fp_0_0 (rc=134) when applying umbrella dnsencrypt to profile.

Caveat ID Number	Description
CSCwb03455	Inter-vrf route leaking not working and packet drop seen due to IPv4 unclassified.
CSCwf03193	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine.
CSCwa43562	Link goes err-disabled due to link-flap after reloading peer device.
CSCwf80400	IOS XE router may experience unexpected reset while executing show utd engine standard statistics .
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface.
CSCwe39011	GARP on port up/up status from router is not received by remote peer device.
CSCvy54048	CPP unexpected reboot while freeing CVLA chunk.
CSCwh26218	Ce0/2/0 DDR: No free dialer - starting fast idle timer.
CSCwb78173	CSDL failure: IPSec QM use of DES by encrypt proc is denied.
CSCwf48808	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
CSCwa69101	Initiator unclassified IP address LQipv4 command has no effect.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwb18108	Unable to boot due to TAM Status TAM_LIB_ERR_WRITE_FAILURE.
CSCwe60059	Crash when using dial-peer groups with STCAPP.
CSCwa76570	ISG/crashes due to %IDMGR-3-INVALID_ID: bad id in id_delete during session roaming.
CSCwc39865	Subscriber session getting stuck and needs clearing it manually.
CSCvz89354	Router running crashes due to CPUHOG when walking ciscoFlashMIB.
CSCvz63684	EWC HA pair experiencing IOS tracebacks, followed by KEYMAN crash.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.

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

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.7

Caveat ID Number	Description
CSCwd30578	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
CSCwa98617	Memory leak in AEM chunks related to firewall.
CSCwb61073	BQS Failure - QoS policy is missing in hardware for some virtual-access tunnels after session flaps.
CSCwa67851	Router traceback and reload when different encapsulation used on xconnect interfaces.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwc76044	Interface stats are not getting updated for port-channel

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.6

Caveat ID Number	Description
CSCwb23043	MACSEC not working on subinterfaces using dot1q >255 between devices.
CSCwc06967	IOS PKI client uses incorrect search filter for CRL retrieval using LDAPv3.
CSCvz92994	Lack of MAC address in inform event message.
CSCwc13013	IPSec key engine process holding memory continuously and not freeing up.
CSCwa17720	Router rebooted due to watchdogs after issuing the commands sh crypto mib IPSec commands.
CSCwb65455	Renewing hardware wan edge cert shows old cert serial/valid date in control local-properties.
CSCwb85046	Device reloads when group-range is configured under an interface group-async.
CSCwb91026	Traffic is hitting wrong sequence in the data policy.
CSCwa66916	SCCP auto-configuration issues with multiple protocols.
CSCwb25913	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwb04815	NHRP process taking more CPU with ip NHRP redirect configured.
CSCwa72273	ZBFW dropping return packets from tunnel post device upgrade.
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map.
CSCvy69405	Appnav-XE connections are going as passthrough unsupported.
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored.
CSCwa80826	IOS-XE: Device platforms running - crypto ipsec policy installation fails.
CSCwa67398	NAT translations do not work for FTP traffic in device.
CSCwa51443	Incorrect check of the TCP sequence number causing return ICMP error packets to drop (Thousandeyes).
CSCwb24123	Registration of spoke fails with dissimilar capabilities w.r.t to HUB.
CSCvw16093	Secure key agent trace levels set to noise by default.
CSCwa84919	"Revocation-check crl none" does not failover to NONE DNAC-CA.
CSCvu70609	Observed crash in device image.
CSCwb15331	Keyman memory leak using public keys.
CSCvy30606	Device fails to update sdn-network-infra-iwan key after 1 year.
CSCwb76988	IKEv2 fragmentation causes wrong message ID used for EAP authentication.

Caveat ID Number	Description
CSCwb99793	CRL verification failure result 400 Bad Request with DigiCert.
CSCvz34668	Static mapping for the hub lost on one of the spokes.
CSCwb95559	Packet sanity failed for resolution reply on spoke due to missing SMEF capability.
CSCwa68540	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
CSCwb72336	ICMP traceroute return packet not classified based on FW override port info.
CSCwa76570	ISG / crashes due to %IDMGR-3-INVALID_ID: bad id in id_delete during session roaming.
CSCvx94323	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut.
CSCwa43562	Device link goes err-disabled due to link-flap after reloading peer device.
CSCwb66749	When configuration ip nat inside/outside on VASI interface, ack/seq number abnormal.
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map.
CSCwa13553	QFP core due to NAT scaling issue.
CSCvy79601	Device gets rebooted when tunnel move across two egress interfaces with QoS MPoL policy config.
CSCwa69101	ISG: Initiator unclassified ip-address LQipv4 command has no effect.
CSCvz53819	ZBFW : ARStandby drops seen on new active during RG switchover.
CSCvz63684	EWC HA pair experiencing IOS tracebacks, followed by KEYMAN crash.
CSCwc22314	Device RTSP traffic not being rewritten by NAT.
CSCwb17282	Router crashing when clearing a VPDN session.
CSCvx74212	IKEv1 IPsec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ.
CSCwb08057	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
CSCwc25291	NIM-LTE-EA no data - requires subslot reload to recover.
CSCwb14888	Unable to remove "switchport mode access" and "switchport nonegotiate" at the same time.
CSCwb12647	Device crash for stuck threads in cpp on packet processing.

Caveat ID Number	Description
CSCwc39865	Subscriber session getting stuck and needs clearing it manually.
CSCwa57462	The router reload unexpectedly due to Cellular CNM process.
CSCvt62123	DMVPN - after removing IPSec, traffic is dropped on a tunnel interface.
CSCwb41907	CPP uCode crash due to ipc congestion from dp to cp.
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface.
CSCvy54048	CPP unexpected reboot while freeing CVLA chunk.
CSCwa76260	IKEv2 deprecated ciphers denied by crypto engine CDSL - PSB security compliance - DES, 3DES, DH1/2/5.
CSCvu77711	Missing mandatory transform type (ESN) in IKEv2 ESP protocol.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwc30050	UTD: Exception in utd_logger.py due to missing extra-data in AMP alert.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCvx28426	Router may crash due to Crypto IKMP process.

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.5

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

Caveat ID Number	Description
CSCwa15132	DMVPN over DMVPN with IPSEC - return packets are dropped with BadIpChecksum
CSCvy68270	CWMP wrong parameter value
CSCvv38438	Watchdog timeout due to Crypto IKMP
CSCwa36699	Prefetch CRL Download Fails
CSCvx39529	IKEv1/IKEv2 show crypto session brief output empty
CSCvt66541	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
CSCvv81296	Protocol specific change for base path
CSCvx94323	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut
CSCvw87352	Missing Serial Number in DSLAM Inventory Check
CSCwa58911	Removing service-policy from the Zone-pair causes device crash
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
CSCvy79601	Device gets rebooted when Tunnel move across two egress interfaces with QoS MPoL policy config
CSCwa17720	Router rebooted de to watchdogs after issuing the commands sh crypto mib ipsec commands
CSCvy26572	[SWI : #01080538] LTE is not reestablishing after reset of the modem
CSCwa50054	Boot Levels Incorrectly Set when Legacy Traditional Licenses are Installed with Smart Licensing
CSCvz53819	ZBFW: ARStandby drops seen on New Active during RG switchover
CSCwa34648	Incorrect OMP Labels in On-Demand Tunnel H/S Topology
CSCwa49902	MGCP automatic configuration fails after IOS-XE upgrade on ISR4k
CSCvx64449	%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: mac verify failed due to ip rtp header-compression iphc-format
CSCvw13048	Crash observed at NHRP while using summary-map
CSCvx74212	IKEv1 IPsec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ
CSCwa51837	Crash on cpp process when QoS policy configuration is being applied

Caveat ID Number	Description
CSCwa18588	IOSd Nhrp core due to a segmentation fault when disabling PfR IWANs
CSCvt62123	DMVPN - after removing IPSec, traffic is dropped on a tunnel interface
CSCwa51443	Incorrect check of the TCP sequence number causing return ICMP error packets to drop (Thousandeyes)
CSCvy47279	Device crashed when PPPoE(running NAT) cable pulled out
CSCwa58533	Unexpected reboot with Critical process fman_fp_image fault on fp_0_0
CSCvu77711	Missing Mandatory Transform Type (ESN) in IKEv2 ESP Protocol
CSCvy41947	EIO: Packets getting reassembled and are forwarded as it is to the Gigabit interface
CSCvy30606	Device: sdn-network-infra-iwan key does not update successfully under network disruption situation
CSCvv55742	GETVPN-ipv6 & LISP support on C900 platforms
CSCwa29964	SCEP fails if AAAA DNS reply is received and source interface has no IPv6 address
CSCwa57462	The router reload unexpectedly due to Cellular CNM process.
CSCwa61238	FlexVPN per-user inline ACL from Radius not installed
CSCvx28426	Router may crash due to Crypto IKMP process

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.4a

Caveat ID Number	Description
CSCvv92064	App-aware policy need to be honored when queuing is not set by localized policy
CSCvw05211	Pre-mature session deletion leading to churn and lower TPS at scale
CSCvw23197	BFD sessions go down on Service VPN after UTD is enabled on cEdge
CSCvw81572	Multiple crashes cpp_cp_svr and qfp-ucode on 16.12.4
CSCvw87300	IP address not correctly in SIP traffic
CSCvx02009	cEdge running 17.3.2 crashed - Critical software exception / IOSXE-WATCHDOG: Process = SNMP ENGINE
CSCvx21270	SDWAN custom policy that does not looked to be programmed correctly on the cedge platform
CSCvx23159	FW-4-ALERT_ON: (target:class)-():getting aggressive seen when no half open feature configed
CSCvx29856	Port mapping NAT configurations not saved to startup config

Caveat ID Number	Description
CSCvx32670	Wrong reload reason reflected after a power outage.
CSCvx36146	DCHP offer frame getting dropped on cEdge ISR4431 due to Policy
CSCvx36205	Removing and Adding Bulk ACL leads to dataplane programming failure
CSCvx36763	Zone Based Firewall on cEdge router dropping web traffic with the reason Zone-pair without policy
CSCvx38454	ISR Crash for CENT-MC-0 process
CSCvx45788	cannot apply ciscosdwan.cfg due to vpg-log-server-acl ACL on VirtualPortGroup0 for logging
CSCvx49102	PPPoE model enablement on CWMP
CSCvx53049	Crash when TPOOL is updating and 'wr mem' is issues at same time
CSCvx55296	CWMP: WANIPConnection.ExternalIPAddress sent in inform instead of WANPPPConnection.ExternalIPAddress
CSCvx55322	CWMP configures PPP chap callin when username is configured
CSCvx57615	ZBFW blocking ACK packets for applications using clouDEXpress SaaS set to use a Gateway with synsent
CSCvx64846	"show sdwan policy service-path/tunnel-path" command cause device crash
CSCvx73741	custom app not getting detected after attached removed and re-attached- app-visibility is disabled
CSCvx75352	CWMP port mapping description is lost after CPE reload
CSCvx77203	[17.5] Router crashed when sending traffic through non-SDWAN interface with DIA NAT + debug enabled
CSCvx78215	An IOS XE device might crash at DoubleExceptionVector
CSCvx79113	SDWAN cedge : traffic simulation tool shows traffic blackhole
CSCvx88246	Packets dropped due to firewall + data policy interop issue
CSCvx89710	SCEP: CA server fails to rollover CA certificate with error: "Storage not accessible"
CSCvx97718	vtcp frees rx buffer when packet with expected next sequence arrives with no payload; phones reset
CSCvy03589	CWMP : Port mpping not created under WANPPP profile when WAN connection is set to PPP Dialer
CSCvy17964	Traceback seen when cwmp wan default interface changed
CSCvy25957	Security container is dropping legitimate FIN,ACK Packets

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

Open Caveats in Cisco IOS XE Amsterdam 17.3.4a

Caveat ID Number	Description
CSCvt62123	DMVPN - after removing IPSec, traffic is dropped on a tunnel interface
CSCvu06483	Data consistency errors seen on configuring mac-sec on the underlay interface with ipsec configured
CSCvv17346	unexpected reload due to Crypto IKEv2 process
CSCvv38438	Watchdog timeout due to Crypto IKMP
CSCvv48885	can not update local-address in a crypto keyring
CSCvw48943	crypto ikev2 proposals are not processed separately
CSCvw60359	cEdge-policy: set next-hop-ipv6 is not working next-hop-ip (ipv4) is working.
CSCvw91361	Crash when issuing "show crypto isakmp peers config"
CSCvw94166	IKE should have a mechanism to alert or mitigate resource exhaustion due to QM flooding
CSCvx74212	IKEv1 IPSec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ
CSCvy10041	Removal of 'set reverse-route tag xxx' removes 'reverse-route' config from crypto map
CSCvy54314	Data-policy local-tloc with app-route is dropping packets when SLA is not met
CSCvy58115	Cedge : Cloudexpress Office 365 probes are hitting 100% loss
CSCvy67301	URL Filtering regex pattern match not working on large pattern
CSCvy68270	CWMP wrong parameter value
CSCvy73818	cEdge QFP starts dropping traffic - UTD Service Node not healthy ident
CSCvy78123	cEdge: High CPU usage due to Multicast and Data Policy configuration.
CSCvy82696	cEdge dropping packets [combination /16, /17 data prefix with multiple ports in policy]
CSCvy69555	Unable to fetch eigrp prefix, nexthop, omptag, and route origin

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.3

Caveat ID Number	Description
CSCuv97577	Mishandling of dsmpSession pointer causes a crash
CSCvu23516	Static routes pointing to interface tunnel not valid after tunnel's source interface flaps.
CSCvu32771	IOSd Crash due to Segmentation fault at SISF Main Thread
CSCvv03229	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
CSCvv09342	Cloud Express probes fails when two default rules are present
CSCvv40006	Traceback: IP SLA triggers INJECT_HDR_LENGTH_ER and INJECT_FEATURE_ESCAPE log message
CSCvv61770	Crash seen in isis_sr_uloop_lspdb_dump with 'debug isis microloop' enabled
CSCvv64633	BGP: advertised community list is malformed due to GSHUT community
CSCvv71775	Cellular interface down/up frequently occurs with DoCoMo MVNO sim
CSCvv78028	No responder-bytes from cEdge when UTD is enabled
CSCvv79273	Router may crash when using Stateful NAT64
CSCvv88621	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage
CSCvv91575	Cisco 1111-8P ISR: NAT translations packet counter MIB OID counts unnecessary additional value
CSCvv91865	Moving PC from network causes static DHCP binding to be removed from the device.
CSCvw06719	"platform ipsec reassemble transit" tail-drops unencrypted IPv4 Fragments with specific payload
CSCvw06780	DMVPN with ipv6 link-local address do not register to HUB
CSCvw09486	Router might crash after apply a class-map in input direction with bandwidth percentage
CSCvw10972	NAT64 ALG: Router crashes on nat64_process_token
CSCvw11902	Passive FTP doesn't work with NAT
CSCvw14131	Crash in TCL Bytecode When Running RA Trace in Guestshell Python
CSCvw14836	ISR router running 16.9.6 crashes authenticating crypto certificate
CSCvw16643	Device Template failing to attach after changing few device variables
CSCvw19171	Smart license registration through explicit mode proxy server
CSCvw19362	[EVPN RT2-RT5] After few host moves RT2-RT5 re-origination happens even when there is no Remote RT2

Caveat ID Number	Description
CSCvw22760	MACSEC MKA stops forwarding data after every 3rd rekey
CSCvw23041	Crash seen on Fugazi due to %CPPHA-3-FAILURE: R0/0: cpp_ha: CPP 0 failure Stuck Thread(s)
CSCvw30128	ip-acl errors of correcting the logic of sequence id when there is an error with msg creation
CSCvw31389	pktlog functionality is broken
CSCvw32481	EVPN Type-2 IP/MAC route is created for not-connected SVI
CSCvw33113	Unexpected reload in NHRP when access to an invalid memory region
CSCvw34157	APPNAV CFT Crashes
CSCvw36514	cEdge crashes due to a large packet at vesen_ipsec_v4_input_get_vctrl_data
CSCvw36629	cEdge: NATed tuple flips for HSL deleted flow
CSCvw37109	Pseudowire interface may be unexpectedly removed from VFI on unrelated configuration change
CSCvw38433	OMP-Agent Routes in EIGRP changes AD to 252 on non-SDWAN devices
CSCvw39383	CPP ucode crash with fw_base_flow_create
CSCvw41482	SSH with Certificate authentication doesn't work after upgrade to 17.3.1
CSCvw47800	HSL Export over VASI Interface causes Netflow v9 Template Flooding
CSCvw48800	unable to transfer 1500 byte IP packet when using BRI bundled Multilink
CSCvw48811	RP went down due to __be_iosd_rec_malloc_free_before
CSCvw54076	[SIT]: BFD sessions not established between Edges, with UTD enabled
CSCvw55030	Dynamic Nat pool "ip aliases" are not created on the device
CSCvw56517	LMR Unable to hear first seconds of audio
CSCvw57860	Duplicate entries seen in MAC filter table.
CSCvw58560	FlexVPN reactivate primary peer feature does not work with secondary peer tracking
CSCvw58646	cEdge: Inspect rule cannot be modified to accept or drop without deactivating the policy
CSCvw62805	SDWAN ZBFW CPU punted traffic mishandling -- Out2In packet looped
CSCvw76715	OpenSSL vulnerability (CVE-2020-1971) evaluation for IOS-XE
CSCvw77485	Router may not send PIM Register message if RP is reachable over TE tunnel

Caveat ID Number	Description
CSCvw80173	BGP AS-path prepend: cEdge won't update correctly better prepended route.
CSCvw84759	Device is crashing after Device Access Policy is attached
CSCvw84883	DDNS feature triggers crash on 16.X/17.X releases due to memory corruption
CSCvw86295	Crash while configuring l2vpn evpn instance for VXLAN
CSCvw97748	Decouple mac aging from ARP aging on vlans not using the centralized gw feature
CSCvx02515	BGP IPv6 link-local session doesn't come up
CSCvx08852	Not able to create VFI instances
CSCvx12686	Memory Lock and system crashed while clearing ip access-list stats.
CSCvx19135	ISR crashes when ZBFW ALG inspects tunneled packet
CSCvx19209	ISIS crash in isis_sr_tilfa_compute_protection
CSCvx36844	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
CSCvw88098	cEdge crashes while running web traffic testing with security features enabled
CSCvw89001	LTE interface is not getting IP address after upgrading the router.
CSCvw89147	Crash at the moment of calculating tcp header
CSCvw92643	Netflow crash at fnf_ipv6_output_feature_final_internal with flow record on IPv6 IPsec tunnel.
CSCvw96723	CP process crashed while I95 driver was adding an IPC response to the receive ring
CSCvx02009	cEdge running 17.3.2 crashed - Critical software exception / IOSXE-WATCHDOG: Process = SNMP ENGINE
CSCvx14095	NETCONF ACL not working if ACL is referencing an object-group.
CSCvx18526	Clients using DHCP Server Port-Based Address Allocation not getting IP address.
CSCvx24332	ucode crash with firewall timer lock
CSCvx24707	bgp-neighbor down when push banner configuration failure
CSCvx25680	IOS-XE Memory Leak in SSS Manager
CSCvx26652	Router crash observed when AppNav Cluster delete with service-insertion enabled on LAN interface

Caveat ID Number	Description
CSCvx35902	fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (Op, Oc) download to FP failed resulting in a crash.
CSCvx38454	ISR Crash for CENT-MC-0 process
CSCvx40030	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
CSCvv85766	Memory leak upon ssh/scp connections to a router
CSCvj29514	CME: Toll fraud app not automatically trusting traffic from phones
CSCvp73666	DNA - LAN Automation doesn't configure link between Peer Device and PnP Agent due CDP limitation
CSCvq65366	Cube might crash when sending a SIP message over TLS
CSCvq73575	TCP traceroute - response ICMP TTL exceeded packet dropped by ZBFW with NAT enabled
CSCvq90343	Secure SIP trunk between SIP-GW/CUBE and CUCM with multiple nodes not coming in to service.
CSCvq97906	"DHCPD Receive" process crash
CSCvq98999	Crash when IPSEC SA installation fails @ imgr_ipsec_sa_n2_install_done
CSCvq99498	Crashes when trying to bring-up / bring-down IPsec crypto session for OSPFv3
CSCvr01327	incorrect Total number of translations on show ip nat translations
CSCvr01454	Punt fragment crash when receive EoGRE packets which have many fragments
CSCvr05213	Smart licensing PID and SN logs filling up the IOSRP tracelogs
CSCvr05504	Dialer interface counter does not correlate to the counter of interfaces bounded to
CSCvr12455	KPML dialing fails after CSCvq20936 commit
CSCvr13358	STUN packet breaks MOH RTP packet flow
CSCvr13385	CUBE/LGW: STUN Indication packets generated constantly for call forking flows
CSCvr17169	qfp ucode crash with media monitor
CSCvr24316	Router crashes due to Segmentation Fault when 'ccb' gives a NULL Pointer
CSCvr26524	Crash due to NBAR classification

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

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

Caveat ID Number	Description
CSCvv94834	BGP crash during IOL testbed launch

Open Caveats in Cisco IOS XE Amsterdam 17.3.2

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

Resolved Caveats in Cisco IOS XE Amsterdam 17.3.1

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

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

Open Caveats in Cisco IOS XE Amsterdam 17.3.1

Caveat ID Number	Description
CSCvv02180	C1113-8PLTEEAWA failed to boot: Package does not support : PID not supported in 17.4
CSCvu59956	IOS cannot boot with 16.12(1r) or later rommon due to cookie PID field incorrectly programmed
CSCvu92277	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.

