



# Release Notes for Cisco Catalyst 8000V Edge Software, Cisco IOS XE Bengaluru 17.6.x

---

**First Published:** 2021-08-16

**Last Modified:** 2024-10-18

## 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)

## Cisco Catalyst 8000V Edge Software Overview

### About Cisco Catalyst 8000V

Cisco Catalyst 8000V Edge Software or Cisco Catalyst 8000V is a software-based, virtual router that combines the functionalities of Cisco Cloud Services Router (Cisco CSR1000V) and Cisco Integrated Services Virtual Router (Cisco ISRv) into a single image that is intended for deployment in on-prem branches, data centers, colocation data centers, and public clouds.

Cisco Catalyst 8000V supports NIM modules on Cisco ENCS platforms, runs on any x86 platform, and is supported on ESXi, KVM, NFVIS hypervisors. Further, you can deploy this router on public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba Cloud.

When you deploy Cisco Catalyst 8000V as a VM, the Cisco IOS XE software behaves similar to a traditional Cisco router (hardware platform). You can configure different features depending on the Cisco IOS XE software version.

### Features

- **Hardware independence:** The Cisco Catalyst 8000V router uses the benefits of virtualization in the cloud to provide hardware independence. Since the Cisco Catalyst 8000V runs as a virtual machine, you can use this router on any x86 hardware that the virtualization platform supports.
- **Sharing of host hardware resources:** The host server hardware resources such as CPU cores, memory, and disk are managed by the hypervisor, and these resources are shared among the guest VMs. You can regulate the amount of hardware resources assigned to a specific Cisco Catalyst 8000V VM instance.
- **Flexibility in deployment:** You can easily move a VM from one server to another. Thus, you can move a Cisco Catalyst 8000V instance from a server in one physical location to a server in another physical location without moving any hardware resources.
- **Enhanced software security - Secure Object Store:** In Cisco Catalyst 8000V, storage partitions for NVRAM, licensing, and other data are created as object stores. The individual object stores are encrypted to ensure data security, and this product is Cisco Secure Development life cycle (CSDL) compliant. Further, Cisco Catalyst 8000V supports a 16G disk profile.

## Hardware Requirements

For hardware requirements and installation instructions, see the [Cisco Catalyst 8000V Edge Software Installation And Configuration Guide](#).

## Software Images and Licenses

The following sections describe the licensing and software images for Cisco Catalyst 8000V.

## Cisco Catalyst 8000V Software Licenses

The Cisco Catalyst 8000V is licensed based on throughput, feature-set, and the licensing term. This product supports Cisco Smart Licensing Usage Policy as well as Cisco DNA Licensing. Based on whether you want to opt for purchased licenses that go with the Cisco Catalyst 8000V instance, or a subscription-based license, choose one of the following options:

### Subscription-Based Licensing via Cisco DNA

You can purchase a subscription license for Cisco Catalyst 8000V through the following three licenses that are available via Cisco DNA:

- Cisco Catalyst 8000V - Network-Advantage
- Cisco Catalyst 8000V - Network-Essentials

For more information on Cisco Catalyst 8000V DNA licensing, see [Cisco DNA Software for SD-Wan and Routing Ordering Guide](#).

### Bring-Your-Own-Licensing

You also have an option to purchase and use licenses with Cisco Catalyst 8000V as a Bring-Your-Own-License (BYOL) instance or as a Pay-As-You-Go (PAYG) instance.

To use a Cisco Catalyst 8000V - BYOL license, see [Licenses and Licensing Models](#) to know to how install and configure your license.

If you have upgraded to Cisco Catalyst 8000V from a Cisco CSR 1000V or a Cisco ISR/V, you must use Smart Licensing Using Policy (SLP). Traditional licenses do not work after the upgrade.

### Pay-As-You-Go Licensing

Cisco Catalyst 8000V supports the PAYG Licensing model with Amazon Web Services (AWS) and Microsoft Azure Marketplace. Cisco Catalyst 8000V hourly-billed AMI or Pay As You Go licensing model allows you to consume an instance for a defined period of time. In this licensing model, you can directly launch the instance from the AWS or Azure Marketplace and start using the instances. The licenses are embedded in the image.



---

**Note** For demo or evaluation licenses, contact your Cisco Account Team if you have a direct purchase agreement with Cisco, or your Cisco Partner or Reseller.

---

For a more detailed overview on Cisco Licensing, go to <https://cisco.com/go/licensingguide>.

## Software Image Nomenclature for Installation Files

The Cisco Catalyst 8000V installation file nomenclature indicates properties supported by the router in a given release.

For example, these are filename examples for the Cisco IOS XE Bengaluru 17.4.1a release:

- c8000v-universalk9.17.04.01a.ova

- c8000v-universalk9.17.04.01a.iso
- c8000v-universalk9.17.04.01a.qcow2

The following table lists the filename attributes along with its properties:

**Table 1: Installation Filename Attributes**

Filename Attribute	Properties
universalk9	Specifies the package that you are installing.
17.04.01a	Indicates that the software image is mapped to the Cisco IOS XE Bengaluru 17.4.1a release.

## Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see <https://www.cisco.com/c/en/us/support/web/field-notice-overview.html>.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from <https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories>.

## New and Enhanced Features in Cisco IOS XE Bengaluru 17.6.x

### New and Changed Software Features in Cisco IOS XE 17.6.8a

There are no new software features in this release.

### New and Changed Software Features in Cisco IOS XE 17.6.7

There are no new software features in this release.

### New and Changed Software Features in Cisco IOS XE 17.6.6a

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 17.6.6

There are no new software features in this release.



---

**Note** See the [End-of-Sale and End-of-Life Announcement for the Cisco IPsec Static Crypto Map and Dynamic Crypto Map Feature in IOS XE](#) page for information about the end-of-life milestones for the Cisco IPsec Static Crypto Map and Dynamic Crypto Map feature.

---

## New and Changed Software Features in Cisco IOS XE 17.6.5a

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 17.6.5

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.6.4

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.6.3a

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.6.2

There are no new software features in this release.

## New and Changed Software Features in Cisco IOS XE 17.6.1a



---

**Note** Cisco IOS XE Bengaluru 17.6.1a is the first release for Cisco Catalyst 8000V in the Cisco IOS XE Bengaluru 17.6.1 release series.

---

The following are the new Cisco Catalyst 8000V software features for Cisco IOS XE Bengaluru Release 17.6.1a:

Table 2: Software Features in 17.6.1a

Feature	Description
<a href="#">AWS Metadata Version 2</a>	Earlier, when you deployed Cisco Catalyst 8000V on Amazon Web Services, only version 1 or V1 was applicable for the <b>Metadata Accessible</b> field. Starting from Cisco IOS XE Release 17.6.1a, metadata version 2 or V2 is also supported. Now, you can either select the V1 and V2 (token optional) option or the V2 (token required) option. When you select either of these options, the instance uses session-oriented requests by creating tokens. The tokens are then used to fetch all the required metadata for your instances.
<a href="#">Automatic Mapping of Cisco CSR 1000V or Cisco ISRV Licenses to DNA Tier Licenses</a>	The Cisco Smart Software Manager (CSSM) manages licenses of all the Cisco devices including Cisco CSR 1000V and Cisco ISRV, which have an end-of-life milestone of year 2022. To continue to keep your Smart Account active, it is mandatory to move to Cisco DNA tier-based licenses. After you activate your Cisco DNA license, CSSM automatically maps the device licenses (CSR 1000V or Cisco ISRV) to your Cisco DNA tier license.
Support for ESXi 7.0	Cisco Catalyst 8000V supports ESXi 7.0 and 6.7 from Cisco IOS XE 17.6.1a. Note that support for ESXi 6.5 has been deprecated.
<a href="#">Zone-Based Firewall Policy Reclassification</a>	The Zone-Based Firewall (ZBFW) Policy Reclassification feature is an enhancement to the Zone-Based Firewall feature. With this enhancement, any changes you make to the policy configuration on an existing firewall session is immediately enforced.
<a href="#">Asymmetric Lease for DHCPv6 Relay Prefix Delegation</a>	This feature allows you to manage or change the lease renewal. It provides options to force renewal of lease and also detects when the lease is nearing the expiry date.
Upgrade to pyang version 2.x	The updated pyang plugin version 2.x fixes existing issues such as XPATH validation and upstream pyang issues. Additionally, this version reports all errors in the YANG models to the users and enforces a strict model validation.

Feature	Description
<a href="#">WebSocket Based Forking for Cloud Speech Services in CUBE</a>	From Cisco IOS XE Bengaluru 17.6.1, CUBE can use WebSockets to handle media forking in a Cisco Unified Contact Center Enterprise (UCCE) solution deployment with Cloud Speech Services. WebSockets transport multiple media streams over a single reliable TLS connection that may traverse firewalls without the need for special policies. WebSocket traffic is also compatible with HTTP load balancers and proxies.
<a href="#">Support for OPUS Codec Transcoding in CUBE</a>	From Cisco IOS XE 17.6.1 onwards, CUBE can transcode Opus encoded media streams. Because Opus codecs perform very well over the Internet, this feature is particularly beneficial when routing calls between the PSTN and Cloud calling services. See also <a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_transcoding.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cube/ios-xe/config/ios-xe-book/m_transcoding.html</a> .
<a href="#">Class of Restriction YANG Configuration Model updates:</a>	YANG models were developed for the following CLIs as part of the Class of Restriction configuration: <ul style="list-style-type: none"> <li>• dial-peer voice &lt;tag&gt; pots/voip corlist</li> <li>• dial-peer voice vad</li> <li>• dial-peer cor custom name &lt;string&gt;</li> <li>• dial-peer cor list &lt;string&gt; member &lt;string&gt;</li> <li>• voice num-exp &lt;string1&gt; &lt;string2&gt;</li> <li>• voice register pool &lt;string&gt; [no] cor {incoming   outgoing} cor-list-name {cor-list-number starting-number [- ending-number]   default}</li> </ul>

Table 3: Software Features in 17.6.2

Feature	Description
Snapshots for PAK Licenses	The library that manages product activation key (PAK) licenses is being deprecated from the software image. To continue supporting and honouring any existing PAK licenses you may have, the system automatically takes a snapshot of the PAK license and triggers a Device-Led Conversion process, to convert the PAK license to a Smart License. For the system to take the snapshot, the software version running on your device must be one of the required releases. For information about the releases in which the system can take a snapshot, and the options that are available with respect to the device and the license, see <a href="#">Snapshots for PAK Licenses</a> .



**Note** From Cisco IOS XE Bengaluru 17.6.x, configuring a weak crypto algorithm generates a warning. But this warning can be safely ignored and does not impact the working of the crypto algorithms. For more information on weak crypto algorithms, see [Supported Standards](#).

## Resolved and Open Bugs for Cisco IOS XE Bengaluru 17.6.x

### Resolved Bugs in Cisco IOS XE 17.6.8a

There are no resolved bugs for this release.

### Open Bugs in Cisco IOS XE 17.6.8a

There are no open bugs in this release.

### Resolved Bugs - Cisco IOS XE 17.6.7

Identifier	Headline
<a href="#">CSCwh73350</a>	Device keeps crashing when processing a firewall feature
<a href="#">CSCwh99399</a>	FTMD crash observed in ENCS platform while running PWK suite
<a href="#">CSCvo01546</a>	NHRP reply processing may dequeue an unrelated request
<a href="#">CSCwh49644</a>	CSDL Compliance failure: Use of 3DES by IPSec is denied
<a href="#">CSCwi01046</a>	PoE module does not provide enough power to bring the ports after an unexpected reload
<a href="#">CSCwh01425</a>	ITU channel configuration does not work



Identifier	Headline
<a href="#">CSCwh20577</a>	Crashed by TRACK client thread at access; invalid memory location
<a href="#">CSCwh70449</a>	PMTUD incorrectly converges without attempting to learn a higher MTU
<a href="#">CSCwf34171</a>	The <b>configure replace</b> command fails due to the <code>license udi PID XXX SN:XXXX</code> line on IOS-XE devices
<a href="#">CSCwh36801</a>	Crash in IP input process during tunnel encapsulation

## Open Bugs - Cisco IOS XE 17.6.7

There are no open bugs in this release.

## Resolved Bugs in Cisco IOS XE 17.6.6a

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 Bugs - Cisco IOS XE 17.6.6a

Identifier	Headline
<a href="#">CSCwe92277</a>	Performance degradation on C8000V hosted in Azure cloud when the traffic flow is asymmetrical
<a href="#">CSCvz96485</a>	Azure: C8000V NETVSC PMD DPDK Support
<a href="#">CSCwe37016</a>	The output rate on the port channel does not match the total physical interface output rate
<a href="#">CSCwh14083</a>	High CPU due to MPLS MIB poll
<a href="#">CSCwd16559</a>	ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table
<a href="#">CSCwf99647</a>	SRTP cipher failure for RTCP packets when AEAD_AES_256_GCM Cipher is used for call
<a href="#">CSCwh21376</a>	Unable to disable the call-home feature on devices
<a href="#">CSCwe93070</a>	Tracebacks seen when configuring VRF with 32 characters or more
<a href="#">CSCwf80400</a>	IOS XE Router may experience unexpected reset while executing the <b>show utd engine standard statistics</b> command
<a href="#">CSCwd46688</a>	Unable to apply the Service Policy on tunnel interfaces

Identifier	Headline
<a href="#">CSCwf55243</a>	Device is crashing while adding a trustpoint to the router
<a href="#">CSCwe29301</a>	AOM objects (FMAN_OBJ_ACL_REF) might be missing intermittently after MMA flapping
<a href="#">CSCwe90119</a>	Device-tracking database entry stuck on UNKNOWN state with temporal mac address.
<a href="#">CSCwh15021</a>	QFP crash when configuring S2S VPN (IKEv2/IPSEC) with Azure vWAN/HUB
<a href="#">CSCwf55145</a>	SFP transceiver DOM does not work after some time; however interface forwards the traffic as expected
<a href="#">CSCvu85539</a>	Unable to delete wrong interface name in C8000V
<a href="#">CSCwd97212</a>	UNIX-EXT-SIGNAL: Segmentation fault(11), Process = IOSXE-RP Punt Service Process
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication
<a href="#">CSCwc67429</a>	CTS PI changes for adding new binding source priority for LISP sourced local host bindings
<a href="#">CSCwh45169</a>	Unexpected reboot while displaying information from a cleared SSS session
<a href="#">CSCwb99084</a>	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
<a href="#">CSCwh49644</a>	CSDL Compliance failure : Use of 3DES by IPsec is denied
<a href="#">CSCwb89958</a>	Unified Policy HSL does not send NBAR application information
<a href="#">CSCvz68895</a>	Device crashes after adding trustpoint
<a href="#">CSCwh42119</a>	Ucode crash when ZBFW is configured on inside interfaces
<a href="#">CSCwf95535</a>	Intf/System xml files are not generated
<a href="#">CSCwf99947</a>	Crash when modifying tunnel after running the <b>show crypto</b> commands
<a href="#">CSCvy94747</a>	GRACEFUL-RELOAD: Wrong state: 1 to receive chasfs event:
<a href="#">CSCwf34171</a>	The <b>configure replace</b> command fails due to the <b>license udi PID XXX SN:XXXX</b> line on IOS-XE devices
<a href="#">CSCwf74668</a>	HSEC licenses incrementing
<a href="#">CSCvz82148</a>	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value
<a href="#">CSCwf80191</a>	Flowspec on device won't revoke
<a href="#">CSCwf41084</a>	Extranet Multicast code improvements for better handling of data structure
<a href="#">CSCwc87565</a>	Unexpected reload due to a watchdog on the kernel

Identifier	Headline
<a href="#">CSCwf00276</a>	Packets with L2TP headers cause device to crash
<a href="#">CSCwd94495</a>	SSM On-Prem responds with message completed to poll_id requests without ACK data
<a href="#">CSCwe85301</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted
<a href="#">CSCwe24491</a>	Static NAT with HSRP stops working after removing / adding standby
<a href="#">CSCwf71557</a>	IPv4 connectivity over PPP not restored after reload
<a href="#">CSCwh01738</a>	Unexpected reload when using rsh/remd
<a href="#">CSCwf59929</a>	CTS CORE process crash after configuring role based ACL
<a href="#">CSCwh35397</a>	Intermittent one way audio on RTP to SRTP calls with SSRC and seq num changes
<a href="#">CSCwh20577</a>	Crashed by TRACK Client thread at access invalid memory location
<a href="#">CSCwe21703</a>	DMI for RESTCONF/NETCONF enters degraded state due to discriminator configured
<a href="#">CSCvz20285</a>	SDWAN image info not updated in packages.conf when upgrading in autonomous mode
<a href="#">CSCwf60120</a>	Static NAT entry gets deleted from running config; but remains in startup config
<a href="#">CSCwf26494</a>	BDI + NTP configuration puts DMI process in degraded mode

## Resolved Bugs - Cisco IOS XE 17.6.6

Identifier	Headline
<a href="#">CSCwf70596</a>	Fix VLAN replay for SRIOV i40e interface after link flap
<a href="#">CSCwe09745</a>	Memory leak in Pubd when continuously trying to connect to remote peer
<a href="#">CSCwd63063</a>	Standby BGP session receives incorrect routes from Active
<a href="#">CSCwe19084</a>	NAT: Traffic is not translated to the same global address though PAP is configured
<a href="#">CSCwd90168</a>	Unexpected reload after running the <b>show voice dsp</b> command while an ISDN call disconnects
<a href="#">CSCwe60059</a>	Crash when using dial-peer groups with STCAPP
<a href="#">CSCwe36122</a>	ISIS crash when performing TI-LFA calculation
<a href="#">CSCwf59173</a>	Segmentation fault at IPv6 BGP backup route notification
<a href="#">CSCwf00769</a>	L2RIB thread crash after removing EVPN member from bridge domain
<a href="#">CSCwf83301</a>	Device displays incorrect values for Call Quality statistics(RTT/MOS)

Identifier	Headline
<a href="#">CSCwe72462</a>	Username/Password under voice register pool gets deleted post CME reload
<a href="#">CSCwe25006</a>	An unexpected removal of the underlay S,G entry resulting ~20s disruption in the multicast flow SDA
<a href="#">CSCwe21042</a>	NBAR DP traceback - "Failed to process non-graph batch message: wrong batch id" is logged
<a href="#">CSCwf47796</a>	NHRP cache entries flood matching a /32 default route
<a href="#">CSCwe32862</a>	Router IOS-XE crashes while executing AES crypto functions
<a href="#">CSCwf09758</a>	Watchdog crashes while importing a large CRL file into the device
<a href="#">CSCwf67564</a>	Memory Leak at process SSS Manager
<a href="#">CSCvy87339</a>	Telemetry subscription fails to connect to grpc receiver when multiple XPATH changes are made to it
<a href="#">CSCwe41946</a>	DTMF is failing through IOS MTP during call on-hold
<a href="#">CSCvq81894</a>	Check nexthop reachability before installing route for a prefix
<a href="#">CSCwe52796</a>	Intermittent one way audio issue after hold and resume SRTP to RTP
<a href="#">CSCvz12193</a>	SNMPwalk: Authentication failure with MD5 SNMPv3 user
<a href="#">CSCwd09685</a>	Memory leak found via the MLD tool
<a href="#">CSCwe64213</a>	LSPVif removal on OIF for RP discovery group 224.0.1.40 with timing related trigger
<a href="#">CSCwf47563</a>	Device crashes after importing the trustpoint with rsakeypair
<a href="#">CSCwe12194</a>	Auto-Update cycle incorrectly deletes certificates
<a href="#">CSCwe33793</a>	Memory allocation failure with extended antireplay enabled
<a href="#">CSCwd59423</a>	Unexpected reload on device caused by WNCd process after removing a VLAN from a VLAN-GROUP
<a href="#">CSCwc03176</a>	Device crashes when applying a service-policy to a newly created tunnel
<a href="#">CSCwa96399</a>	Configuring entity-information xpath filter causes syslogs to print, does not return data
<a href="#">CSCwh04884</a>	VC Down due to control-word negotiation
<a href="#">CSCwc24044</a>	IOS XE device may experience an unexpected reset with high volume of multicast
<a href="#">CSCwb47153</a>	Keyman process crash
<a href="#">CSCwc99453</a>	Enable the <b>license feature hseck9</b> command
<a href="#">CSCwe18124</a>	Macsec remains marked as SECURED, but randomly the traffic stops working

Identifier	Headline
<a href="#">CSCwb59052</a>	Observe traceback message when BVM client do Inter-xTR roaming
<a href="#">CSCwd73783</a>	Observed qfp-ucode-wlc crash
<a href="#">CSCwf14135</a>	SIPREC recording fails in transfer scenario when certian options are enabled during configuration
<a href="#">CSCwf56463</a>	IOS process crashes during VRRP hash table lookup
<a href="#">CSCwf44649</a>	LISP failed to recreate the more specific away table entries after less specific entries toggled
<a href="#">CSCwe23150</a>	CUBE memory leak sdp_copy_all_attrs sdp_parse_attribute sdp_add_new_attr
<a href="#">CSCwf48808</a>	FlexVPN: Stale Client Routes stuck in RIB on FlexServer
<a href="#">CSCwf39490</a>	MCID (Malicious Call Identification) breaks due to custom prefix setting under STCAPP FAC
<a href="#">CSCwd99921</a>	The IOS XE software crashes while validating certification trust
<a href="#">CSCvy14316</a>	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M)
<a href="#">CSCwe56033</a>	No alarms are triggered when RPM of a fan is 0
<a href="#">CSCwe36743</a>	Segmentation Fault - Crash - SSH - When Changing AAA Group Configs
<a href="#">CSCwe97579</a>	Spoke-spoke cache refresh not working correctly in case of multiple cache entries for same next hop
<a href="#">CSCwf41082</a>	MallocLite Memory Leak observed in HTTP CORE Allocator
<a href="#">CSCwh11858</a>	Switch running IOS-XE crashes when removing FQDN ACL
<a href="#">CSCwe89823</a>	Router crashes due to CPUHOG when walking ciscoFlashMIB @snmp_platform_get_flash_file_info
<a href="#">CSCwf29859</a>	Logging in get-config processing affecting the template push fail
<a href="#">CSCwd28734</a>	Device memory leak in pubd causes switch reload
<a href="#">CSCwf27815</a>	DSP resource can not be released after call ends
<a href="#">CSCuq20562</a>	ISDN memory leak when PRI link flaps, crashes router
<a href="#">CSCwf01986</a>	Radius attribute 31 not being sent on device for CTS Pac provisioning
<a href="#">CSCwf03292</a>	I/O middle pool leaking when VOIP trace is enabled
<a href="#">CSCwe66318</a>	NAT entries expire on Standby Router
<a href="#">CSCwh05407</a>	Gateway disconnecting incoming calls when FPI Correlator is not released after disconnect on PRI Leg

Identifier	Headline
<a href="#">CSCwe39011</a>	GARP on port up/up status from router is not received by remote peer device
<a href="#">CSCwfl4589</a>	IOS-XE device may experience a segmentation fault with L2VPN EVPN when clearing duplicate MAC
<a href="#">CSCwe70237</a>	CUBE reloads due to a segmentation fault in CCSIP_SPI_CONTROL process
<a href="#">CSCwd12330</a>	Invalid TCP checksum in SYN flag packets passing through router
<a href="#">CSCwf24164</a>	Netflow stops working when flow monitor reaches cache limit
<a href="#">CSCwd49177</a>	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packets are switched
<a href="#">CSCwf08698</a>	Device Crashes Unexpectedly due to a fault in the 'TLSCLIENT_PROCESS'

## Open Bugs - Cisco IOS XE 17.6.6

Identifier	Headline
<a href="#">CSCwe92277</a>	Performance degradation on C8000V hosted in Azure cloud when the traffic flow is asymmetrical
<a href="#">CSCvz96485</a>	Azure: C8000V NETVSC PMD DPDK Support
<a href="#">CSCwe37016</a>	The output rate on the port channel does not match the total physical interface output rate
<a href="#">CSCwh14083</a>	High CPU due to MPLS MIB poll
<a href="#">CSCwd16559</a>	ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table
<a href="#">CSCwf99647</a>	SRTP cipher failure for RTCP packets when AEAD_AES_256_GCM Cipher is used for call
<a href="#">CSCwh21376</a>	Unable to disable the call-home feature on devices
<a href="#">CSCwe93070</a>	Tracebacks seen when configuring VRF with 32 characters or more
<a href="#">CSCwf80400</a>	IOS XE Router may experience unexpected reset while executing the <b>show utd engine standard statistics</b> command
<a href="#">CSCwd46688</a>	Unable to apply the Service Policy on tunnel interfaces
<a href="#">CSCwf55243</a>	Device is crashing while adding a trustpoint to the router
<a href="#">CSCwe29301</a>	AOM objects (FMAN_OBJ_ACL_REF) might be missing intermittently after MMA flapping
<a href="#">CSCwe90119</a>	Device-tracking database entry stuck on UNKNOWN state with temporal mac address.
<a href="#">CSCwh15021</a>	QFP crash when configuring S2S VPN (IKEv2/IPSEC) with Azure vWAN/HUB

Identifier	Headline
<a href="#">CSCwf55145</a>	SFP tranceiver DOM does not work after some time; however interface forwards the traffic as expected
<a href="#">CSCvu85539</a>	Unable to delete wrong interface name in C8000V
<a href="#">CSCwd97212</a>	UNIX-EXT-SIGNAL: Segmentation fault(11), Process = IOSXE-RP Punt Service Process
<a href="#">CSCwe14885</a>	VPN is established although the peer is using a revoked certificate for authentication
<a href="#">CSCwc67429</a>	CTS PI changes for adding new binding source priority for LISP sourced local host bindings
<a href="#">CSCwh45169</a>	Unexpected reboot while displaying information from a cleared SSS session
<a href="#">CSCwb99084</a>	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
<a href="#">CSCwh49644</a>	CSDL Compliance failure : Use of 3DES by IPsec is denied
<a href="#">CSCwb89958</a>	Unified Policy HSL does not send NBAR application information
<a href="#">CSCvz68895</a>	Device crashes after adding trustpoint
<a href="#">CSCwh42119</a>	Ucode crash when ZBFW is configured on inside interfaces
<a href="#">CSCwf95535</a>	Intf/System xml files are not generated
<a href="#">CSCwf99947</a>	Crash when modifying tunnel after running the <b>show crypto</b> commands
<a href="#">CSCvy94747</a>	GRACEFUL-RELOAD: Wrong state: 1 to receive chasfs event:
<a href="#">CSCwf34171</a>	The <b>configure replace</b> command fails due to the <b>license udi PID XXX SN:XXXX</b> line on IOS-XE devices
<a href="#">CSCwf74668</a>	HSEC licenses incrementing
<a href="#">CSCvz82148</a>	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value
<a href="#">CSCwf80191</a>	Flowspec on device won't revoke
<a href="#">CSCwf41084</a>	Extranet Multicast code improvements for better handling of data structure
<a href="#">CSCwe87565</a>	Unexpected reload due to a watchdog on the kernel
<a href="#">CSCwf00276</a>	Packets with L2TP headers cause device to crash
<a href="#">CSCwd94495</a>	SSM On-Prem responds with message completed to poll_id requests without ACK data
<a href="#">CSCwe85301</a>	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted
<a href="#">CSCwe24491</a>	Static NAT with HSRP stops working after removing / adding standby

Identifier	Headline
<a href="#">CSCwf71557</a>	IPv4 connectivity over PPP not restored after reload
<a href="#">CSCwh01738</a>	Unexpected reload when using rsh/rcmd
<a href="#">CSCwf59929</a>	CTS CORE process crash after configuring role based ACL
<a href="#">CSCwh35397</a>	Intermittent one way audio on RTP to SRTP calls with SSRC and seq num changes
<a href="#">CSCwh20577</a>	Crashed by TRACK Client thread at access invalid memory location
<a href="#">CSCwe21703</a>	DMI for RESTCONF/NETCONF enters degraded state due to discriminator configured
<a href="#">CSCvz20285</a>	SDWAN image info not updated in packages.conf when upgrading in autonomous mode
<a href="#">CSCwf60120</a>	Static NAT entry gets deleted from running config; but remains in startup config
<a href="#">CSCwf26494</a>	BDI + NTP configuration puts DMI process in degraded mode

## Resolved Bugs in Cisco IOS XE 17.6.5a

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 Bugs - Cisco IOS XE 17.6.5a

Bug ID	Headline
<a href="#">CSCwd79089</a>	Device controller crash when sending full line rate of traffic with >5 Intel AX210 stations
<a href="#">CSCwd90168</a>	Unexpected reload after running 'show voice dsp' command while an ISDN call disconnects
<a href="#">CSCvq81894</a>	Check nexthop reachability before installing route for a prefix
<a href="#">CSCwb99084</a>	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
<a href="#">CSCwb89958</a>	Unified Policy HSL does not send NBAR application information properly
<a href="#">CSCwd07580</a>	Azure: C8000V QFP uCode crash due to MLX4 driver
<a href="#">CSCwd92344</a>	C8000V crash observed in Azure due to Segmentation Fault with MLX5 drivers
<a href="#">CSCwd89338</a>	Clear ISG existing lite-session upon reception of DHCP packet for same client
<a href="#">CSCwd71458</a>	Outgoing number of bytes decrease in router' interface
<a href="#">CSCwd97676</a>	VMware C8000V 'show interfaces' counters are incorrect and display extremely large values
<a href="#">CSCwd49177</a>	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packets are switched



Bug ID	Headline
<a href="#">CSCwe19617</a>	Bash core observed on C8000V in the idle state.

## Resolved Bugs - Cisco IOS XE 17.6.5

Bug ID	Headline
<a href="#">CSCwd47123</a>	ISG uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply
<a href="#">CSCvz93612</a>	%HW_FLOWDB-3-HW_FLOWDB_DBLDEL_FEATOBJ: FlowDB featobj cannot be deleted twice
<a href="#">CSCvy60839</a>	CSDL Compliance: Added a new command to disable weak crypto checking in future releases.
<a href="#">CSCwc82140</a>	QFP Crash When ZBFW configuration features "log dropped-packets" configuration
<a href="#">CSCwc99823</a>	fman crash seen in SGACL@ fman_sgac1_alloc
<a href="#">CSCwc78021</a>	Standby WLC crash @ fman_acl_remove_default_ace
<a href="#">CSCvz92994</a>	Lack of MAC address in the Inform Event message.
<a href="#">CSCwc89328</a>	Device might reboot when supporting explicit IV joins the SD-WAN network
<a href="#">CSCwb52324</a>	C8000V unexpectedly reloads due to QFP ucode crash
<a href="#">CSCwd71584</a>	DSPware 58.5.2 release targeting v176_throttle
<a href="#">CSCwd61255</a>	Data Plane Crash on the device when Making QOS configuration changes
<a href="#">CSCwb04815</a>	NHRP process takes more CPU because of FlexVPN event trace
<a href="#">CSCwc22314</a>	RTSP Traffic not being rewritten by NAT
<a href="#">CSCwd30578</a>	Wired guest client stuck at IP_LEARN with dhcp packets not forwarded out of the foreign to anchor
<a href="#">CSCwd56131</a>	LTE modem doesn't show GSM bands
<a href="#">CSCwb73395</a>	Need CLI option to disable ALG
<a href="#">CSCwc54463</a>	Device LAN module is down when high CPU noticed
<a href="#">CSCwc72923</a>	ERROR info: Router configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt
<a href="#">CSCwc84967</a>	Intermittent double DTMF due to changing timestamp on a DTMF event
<a href="#">CSCwb08057</a>	Number of lite sessions conversion in progress counter not decrementing on failed account-logon
<a href="#">CSCwc29629</a>	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 IPsec crypto session authentication
<a href="#">CSCwc77981</a>	C8000V crashed - track the fman-fp's memory leak caused by cond-debug
<a href="#">CSCwb32635</a>	Device vdaemon file is incomplete when running admin-tech
<a href="#">CSCwd72312</a>	GETVPN : Traffic drops seen on GM after rekey installing policies

## Open Bugs - Cisco IOS XE 17.6.5

Bug ID	Headline
CSCwd79089	Device controller crash when sending full line rate of traffic with >5 Intel AX210 stations
CSCwd90168	Unexpected reload after running 'show voice dsp' command while an ISDN call disconnects
CSCvq81894	Check nexthop reachability before installing route for a prefix
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
CSCwb89958	Unified Policy HSL does not send NBAR application information properly
CSCwd07580	Azure: C8000V QFP uCode crash due to MLX4 driver
CSCwd92344	C8000V crash observed in Azure due to Segmentation Fault with MLX5 drivers
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client
CSCwd71458	Outgoing number of bytes decrease in router' interface
CSCwd97676	VMware C8000V 'show interfaces' counters are incorrect and display extremely large values
CSCwd49177	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packets are switched
CSCwe19617	Bash core observed on C8000V in the idle state.

## Resolved Bugs - Cisco IOS XE 17.6.4

Bug ID	Headline
CSCwb95559	Packet Sanity failed for Resolution Reply on Spoke due to missing SMEF capability
CSCvz93712	VFR is enabled by feature NAT but there is no NAT configured on the interface
CSCwa84919	"Revocation-check crl none" does not failover to NONE DNAC-CA
CSCvz63684	EWC HA pair experiencing IOS tracebacks followed by KEYMAN Crash
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions
CSCwc33311	cEdge crash @ imgr_n2_ipsec_sa_ctx_register
CSCwa33174	Azure C8000V: 'show interfaces' counters are incorrect and display extremely large values
CSCwc06967	IOS PKI client uses incorrect search filter for CRL retrieval using LDAPv3
CSCwc37320	RP Switchover Causes Linecard NFS mount Failure Resulting in Memory Leak
CSCwb05743	Crash seen with umbrella config during soak run
CSCvz83016	BFD tunnel uptime does not show correct values post upgrade
CSCwb43605	OMPd crash during RIB-out attribute aspath/community processing
CSCwc13013	IPSec Key Engine process holding memory continuously and not freeing up
CSCwb34625	C8000V auto mode: static ip from bootstrap config overwritten by dhcp on fresh install

Bug ID	Headline
<a href="#">CSCwb73511</a>	Device is not able to bring up SIG tunnels after reboot
<a href="#">CSCwb91729</a>	Fix mishandling of policy sequence programming failures and notify with syslog/notification
<a href="#">CSCwa67886</a>	UDP based DNS resolution doesn't work with IS-IS EMCP on IOX-XE
<a href="#">CSCwb85046</a>	Device reloads when group-range is configured under an interface Group-Async
<a href="#">CSCwc39881</a>	C8000V generated from hardware cEdge contains "/" in Common Name
<a href="#">CSCvz23982</a>	IOS sending UP Event for the sub interface which is in down state
<a href="#">CSCvx93283</a>	Service Chain is not created when Tracking is disabled
<a href="#">CSCvz99832</a>	Per class BFD - echo response pkts
<a href="#">CSCwb08636</a>	IPSEC-3-HMAC_ERROR: IPsec SA receives HMAC error seen for TLOCExt setup after upgrade
<a href="#">CSCvx74917</a>	DNS packets are not redirected to configured custom DNS after Umbrella template edit
<a href="#">CSCwa72273</a>	ZBFW dropping return packets from tunnel post upgrade
<a href="#">CSCwb32934</a>	Device does not use QAT when malloc failure
<a href="#">CSCwa08378</a>	C8000V Day0 ZTP ignores crypto configuration before licensing
<a href="#">CSCwa64955</a>	Device loses control connections after installing new enterprise hardware wan edge cert
<a href="#">CSCwa92137</a>	Device is changing ICMP ID in ICMP echo, replies intermittently
<a href="#">CSCwa81471</a>	AOM pending objects with loopbacks binded to tloc-extended interfaces
<a href="#">CSCwb49857</a>	Memory leaks on keyman process when key is not found
<a href="#">CSCwb76866</a>	CSDL failure: Use of MD5 by IPSEC key engine is denied
<a href="#">CSCwb55683</a>	Large number of IPsec tunnel flapping occurs when underlay is restored
<a href="#">CSCwa80826</a>	IOS-XE: Devices running crypto ipsec policy experience installation failure
<a href="#">CSCwb83376</a>	Device endpoint-tracker cannot be configured on a 100G interface
<a href="#">CSCwc13304</a>	Per-tunnel QoS counters and shapers not working for some bfd tunnel with stale 'nh_overlay' objects
<a href="#">CSCwa67398</a>	NAT translations do not work for FTP traffic in device
<a href="#">CSCwb78173</a>	CSDL failure: IPsec QM Use of DES by encrypt proc is denied
<a href="#">CSCwb76170</a>	IPsec SIG auto tunnels are not coming up
<a href="#">CSCwb41907</a>	CPP uCode crash due to ipc congestion from dp to cp
<a href="#">CSCvy54048</a>	CPP Unexpected reboot occurs while freeing CVLA chunk
<a href="#">CSCwa30857</a>	Internet SpeedTest with loopback binding mode doesn't work with implicit ACL drop for return traffic
<a href="#">CSCwb14020</a>	Serial interface stuck in "line protocol is down" state after it went down and is recovered
<a href="#">CSCwa98545</a>	Checks of route leaks creates memory corruption

Bug ID	Headline
<a href="#">CSCwb46649</a>	NAT translation does not show (or use) correct timeout value for an established TCP session
<a href="#">CSCwa08847</a>	ZBFW policy stops working after modifying the zone pair
<a href="#">CSCwb58468</a>	Sig Autotunnels:tunnel 409 response received
<a href="#">CSCwa26599</a>	FN980 new signed Telit modem firmware FN980M_38.02.X92 upgrade failed
<a href="#">CSCwb12647</a>	Device crash for stuck threads in cpp on packet processing
<a href="#">CSCwc04688</a>	Device crash observed after enabling NWPI trace with IPv6 traffic
<a href="#">CSCwb76988</a>	IKEv2 fragmentation causes wrong message ID to be used for EAP authentication
<a href="#">CSCvw50622</a>	Nhrp network resolution not working with link-local ipv6 address
<a href="#">CSCwa57873</a>	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request
<a href="#">CSCvz37340</a>	The [service timestamps log datetime msec localtime] command cannot be pushed via CLI Addon template
<a href="#">CSCwb99793</a>	CRL verification failure results in 400 Bad Request with DigiCert
<a href="#">CSCwb90470</a>	Device crashed with last reload reason 'Critical process expd fault'
<a href="#">CSCwb32059</a>	Cellular interface tracker down but NAT route persists in the Service VPN Routing Table
<a href="#">CSCwb51595</a>	Missing IOS config (voice translation rule) on upgrade
<a href="#">CSCwb40575</a>	After upgrade, umbrella dns config set to NONE in show umbrella config
<a href="#">CSCwb18315</a>	Umbrella DNS security policy doesn't work with Cloud onRamp with SIG tunnels
<a href="#">CSCwb13850</a>	License boot level not detected with Day0 after C8000V boots on NFVIS platforms
<a href="#">CSCwc04289</a>	Inconsistency between Path MTU Discovery result and Tunnel MTU

## Open Bugs - Cisco IOS XE 17.6.4

Bug ID	Headline
<a href="#">CSCwc29629</a>	Crashes when Virtual-Access tries to bring-up/bring-down OSPFv3 ipsec crypto session authentication
<a href="#">CSCwc23077</a>	Firewall drop seen stating FirewallL4
<a href="#">CSCvz92994</a>	Lack of MAC address in Inform Event message.
<a href="#">CSCwc50477</a>	Device crashed in ipv4_nat_create_out2in_session_entry
<a href="#">CSCwc55260</a>	Memory leak due to FTMD process
<a href="#">CSCwb99084</a>	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
<a href="#">CSCwb89958</a>	Unified Policy HSL not sending proper NBAR application information.
<a href="#">CSCwc59598</a>	Statistics collection causes service-side BFD to flap on every collection interval
<a href="#">CSCwc22314</a>	RTSP Traffic not being rewritten by NAT
<a href="#">CSCwb83236</a>	Traceback: QFP core after pushing data policy with IPv6 interface

Bug ID	Headline
<a href="#">CSCwc67465</a>	Router cannot be upgraded
<a href="#">CSCwc63563</a>	Unable to set specific speed and duplex values on SFP ports on IOS-XE routing platforms
<a href="#">CSCwc43973</a>	DLC is not completing after upgrading to Smart licensing from CSL
<a href="#">CSCwc30050</a>	UTD: Exception in utd_logger.py due to missing extra-data in AMP alert
<a href="#">CSCwc27208</a>	BFD sessions not coming up because of ANTI-REPLAY-FAILURES
<a href="#">CSCwc25291</a>	NIM-LTE-EA No Data - Requires subslot reload to recover
<a href="#">CSCwd36511</a>	Ping fail to VRRP virtual IP address.

## Resolved Bugs - Cisco IOS XE 17.6.3a

Bug ID	Headline
<a href="#">CSCvy63924</a>	Telemetry: IOS-XE Controller crashes after using 'show telemetry ietf subscription all' command.
<a href="#">CSCwa13553</a>	C8000V QFP core due to NAT scaling issue
<a href="#">CSCvx40516</a>	17.5 ZBFW + NAT: Traffic flow In2Out scenario failed
<a href="#">CSCwa26509</a>	Shut/no shut of endpoint-tracker attached tunnel, doesn't create probe again on 17.6.2
<a href="#">CSCvz98373</a>	ZBFW : FirewallPolicy drops seen with RTSP traffic in steady state
<a href="#">CSCvz71436</a>	Call Placing issue from SCCP phones
<a href="#">CSCvy69846</a>	Guestshell:.py files stored under /home/guestshell are lost after reboot on Ing device
<a href="#">CSCvz86591</a>	VRF-aware static NAT with route-map and reversible not working
<a href="#">CSCwa30988</a>	CoS preservation not working for the services EVPL and EPL tunnel
<a href="#">CSCwa36699</a>	Prefetch CRL Download Fails
<a href="#">CSCvv82985</a>	dhcpv6_relay:dhcp-client on branch not receive ipv6 address
<a href="#">CSCwa76260</a>	IKEv2 Deprecated Ciphers denied by Crypto Engine CDSL - Cisco PSB Security Compliance
<a href="#">CSCvt66541</a>	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted
<a href="#">CSCwa11150</a>	E1 configurations (under Serial interface) lost after reload.
<a href="#">CSCvz65545</a>	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535
<a href="#">CSCvz41647</a>	Partial multicast drops are seen after a failover event in a site with two cedges
<a href="#">CSCvz76277</a>	Hostname not allowed beginning with numbers
<a href="#">CSCvz34668</a>	Static mapping for the hub lost on one of the spokes
<a href="#">CSCvz84437</a>	Unexpected reload due IPV6 UDP fragment header in VxLAN
<a href="#">CSCwa15085</a>	Router Crash due to Stuck Thread with appnav-xe dual controller mode.
<a href="#">CSCvx28426</a>	Router may crash due to Crypto IKMP process

Bug ID	Headline
<a href="#">CSCwa18177</a>	Flapping bidirectional/unidirectional packet capture option with ipv4 filter for long time failed
<a href="#">CSCvy97741</a>	Multiple qfp-ucode crash when making a blind transfer from an outside SIP service

## Open Bugs - Cisco IOS XE 17.6.3a

Bug ID	Headline
<a href="#">CSCvz93712</a>	VFR is enabled by feature NAT but there is no NAT configured on the interface
<a href="#">CSCvy72970</a>	Active ftp not working with UTD+HTX for security and Unified policy.
<a href="#">CSCvz05814</a>	Cwand issue observed ..potential crash
<a href="#">CSCwb25913</a>	After configuring match input-interface on class-map, router goes into a reboot loop
<a href="#">CSCwb03455</a>	Inter-vrf route leaking not working and packet drop seen due to Ipv4 Unclassified
<a href="#">CSCwb32934</a>	QAT is not used during malloc failure
<a href="#">CSCwa08378</a>	C8000V Day0 ZTP ignores crypto configuration before licensing
<a href="#">CSCwb13820</a>	C8Kv crashed at high scale with IPSEC and heavy features configured
<a href="#">CSCwb08186</a>	E1 R2 - dnis-digits cli not working
<a href="#">CSCwb26741</a>	ZBFW performance variance observed with 17.6 images on 8v CPU due to rx_miss errors
<a href="#">CSCwa81471</a>	AOM pending objects with loopbacks binded to tloc-extended interfaces
<a href="#">CSCwa68471</a>	Traceback: CPP ucode core generated after HSRP priority change
<a href="#">CSCvz28950</a>	DMVPN phase 2 connectivity issue between two spokes
<a href="#">CSCwb18223</a>	SNMP v2 community name encryption problem
<a href="#">CSCvy54048</a>	CPP Unexpected Reboot While Freeing CVLA Chunk
<a href="#">CSCwa98545</a>	Checks of route leaks creates memory corruption.
<a href="#">CSCwa76875</a>	After configuring match input-interface on class-map, router goes into a reboot loop
<a href="#">CSCwa08847</a>	ZBFW policy stops working after modifying the zone pair
<a href="#">CSCwa29964</a>	SCEP fails if AAAA DNS reply is received and source interface has no IPv6 address
<a href="#">CSCvz55275</a>	Show DMVPN command displays incorrect state
<a href="#">CSCwa74499</a>	ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection
<a href="#">CSCvz74322</a>	"Shutdown" command visible in running config after reload of instance

## Resolved Bugs - Cisco IOS XE 17.6.2

Caveat ID Number	Description
<a href="#">CSCvz08449</a>	Cat8kv - Incorrect static route for primary interface during deployment resulting in unreachability

## Open Bugs - Cisco IOS XE 17.6.2

There are no open bugs for this release.

## Resolved Bugs - Cisco IOS XE 17.6.1a

Caveat ID Number	Description
<a href="#">CSCvw83359</a>	AWS:C8000V crashed and reboots if shut/no shut an interface a number of times.
<a href="#">CSCvy52270</a>	CSR1000V/C8000V: Console Port Access change CLI does not work in the CONTROLLER mode.
<a href="#">CSCvx86151</a>	ovf-template should give option for DNA essentials, advantage, premier on C8kv deployment in vcenter
<a href="#">CSCvv35440</a>	C8000v WebUI is not accessible by user.

## Open Bugs - Cisco IOS XE 17.6.1a

Caveat ID Number	Description
<a href="#">CSCvx94285</a>	C8000V crashes after oce_lookup_one_adj_id_handle while reading emu_mem.
<a href="#">CSCvz22268</a>	With curl schedule download, stuck Failed to send the request. There is another request in progress.

## Related Documentation

[Cisco Catalyst 8000V Edge Software Product Page](#)

[Cisco Catalyst 8000V Edge Software Data Sheet](#)

[Cisco Catalyst 8000V Edge Software Installation And Configuration Guide](#)

[Cisco Catalyst 8000V Edge Software High Availability Configuration Guide](#)

[Troubleshooting Guide for Cisco Catalyst 8000V Edge Software](#)

[Smart Licensing Using Policy for Cisco Enterprise Routing Platforms](#)

## 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 DevNet](#).
- 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.