Release Notes for Cisco Catalyst 8300 Series Edge Platforms, Cisco IOS XE Bengaluru 17.6.x

First Published: 2021-08-25

Last Modified: 2024-04-04

Full Cisco Trademarks with Software License

About Cisco Catalyst 8300 Series Edge Platforms

The Cisco Catalyst 8300 Series Edge Platforms are best-of-breed, 5G-ready, cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

Cisco Catalyst 8300 Series Edge Platforms with Cisco IOS XE SD-WAN Software deliver Cisco's secure, cloud-scale SD-WAN solution for the branch. The Cisco Catalyst 8300 Series Edge Platforms is built for high performance and integrated SD-WAN Services along with flexibility to deliver security and networking services together from the cloud or on premises. It provides higher WAN port density and a redundant power supply capability. The Cisco Catalyst 8300 Series Edge Platforms have a wide variety of interface options to choose from—ranging from lower and higher module density with backward compatibility to a variety of existing WAN, LAN, voice, and compute modules. Powered by Cisco IOS XE, fully programmable software architecture, and API support, these platforms can facilitate automation at scale to achieve zero-touch IT capability while migrating workloads to the cloud. The Cisco Catalyst 8300 Series Edge Platforms also come with Trustworthy Solutions 2.0 infrastructure that secures the platforms against threats and vulnerabilities with integrity verification and remediation of threats.

The Cisco Catalyst 8300 Series Edge Platforms are well suited for medium-sized and large enterprise branch offices for high WAN IPSec performance with integrated SD-WAN services.

For more information on the features and specifications of Cisco Catalyst 8300 Series Edge Platforms, refer to the Cisco Catalyst 8300 Series Edge platforms datasheet.

Note Sections in this documentation apply to all models of Cisco Catalyst 8300 Series Edge Platforms unless a reference to a specific model is made explicitly.

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)

Note Cisco IOS XE Bengaluru 17.6.1a is the first release for Cisco Catalyst 8300 Series Edge Platforms.

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 Changed Hardware and Software Features

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the software features, platform, and software image support on Cisco Catalyst 8200 and Catalyst 8300 Series Edge Platforms. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/.

Note To access CFN, you do not require an account on cisco.com.

New and Changed Hardware Features

New Hardware Features

- Cisco C-NIM-1M or C-NIM-2T Network Interface Module: The Cisco C-NIM-1M and C-NIM-2T are the next generation 1x2.5mG and 2x1G WAN NIM modules, which is supported on Cisco Catalyst 8300 Series Edge Platforms.
- Cisco Catalyst 8300 Series Edge Platforms support SVTI Dual stack.

For information on the hardware features supported on the NIM-PVDM, refer to the Cisco Packet Voice Digital Signal Processor Modules for Cisco Unified Communications Solutions datasheet.

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

Table 1: New Software Features in Release Cisco IOS XE Bengaluru 17.6.1a

Feature	Description
Asymmetric Lease for DHCPv6 Relay Prefix Delegation	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.
CUBE: OPUS Codec Transcoding	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.
Cisco ThousandEyes Enterprise Application Hosting	Cisco ThousandEyes application is a cloud-ready, enterprise network-monitoring tool that provides an end-to-end view across networks and services. This tool helps in analyzing the network performance and provides insights into the Internet and enterprise networks.
ISR Serviceability: Consistent System-report	This feature lets you configure system reports that can provide critical information on issues that cause software crashes.
L2VPN Traffic Steering Using SR-TE Preferred Path	This feature allows you to configure an SR policy as the preferred path for a VPWS or VPLS pseudowire. VPWS or VPLS pseudowires between same PEs can be routed over different SR policies based on the requirements.
PPPoE Client over VLAN Interface	The PPPoE Client over VLAN interface enhancement allows you to configure the PPPoE client to establish a PPPoE session over a VLAN interface.

Feature	Description
Unified CME: Availability with Catalyst Edge 8300 Platforms	From Cisco IOS XE 17.6.1 onwards, CME is supported on Cisco 8300 Catalyst Edge Series platforms.
Voice: Class of Restriction YANG Configuration Model	YANG models were developed for the following CLIs as part of the Class of Restriction configuration: • dial-peer voice <tag> pots/voip corlist • dial-peer voice vad • dial-peer cor custom name <string> • dial-peer cor list <string> member <string> • voice num-exp <string1> <string2> • voice register pool <string> [no] cor {incoming | outgoing} cor-list-name {cor-list-number starting-number [- ending-number] | default}
Zone-Based Firewall Reclassification	The Zone-Based Firewall (ZBFW) 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.

Note From Cisco IOS XE Bengaluru 17.6.x, configuring a weak crypto algorithm generates a warning message. However, you can ignore this warning because the working of crypto algorithms is *not* impacted. For more information on weak crypto algorithms, see Supported Standards.

Cisco Catalyst 8300 Series Edge Platforms ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.6.x releases.

Table 2: Minimum and Recommended ROMMON Releases Supported on C8300-1N1S-4T2X and C8300-1N1S-6T

Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
17.6.1	17.3(5r)	17.6(6r)

Table 3: Minimum and Recommended ROMMON Releases Supported on C8300-2N2S-4T2X and C8300-2N2S-6T

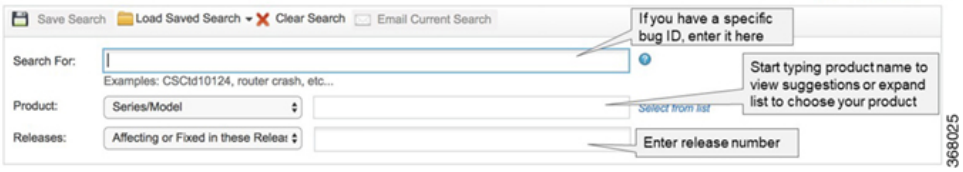
Cisco IOS XE Release	Minimum ROMMON Release Supported for IOS XE	Recommended ROMMON Release Supported for IOS XE
17.6.1	17.3(4.1r)	17.6(6.1r)

Resolved and Open Caveats

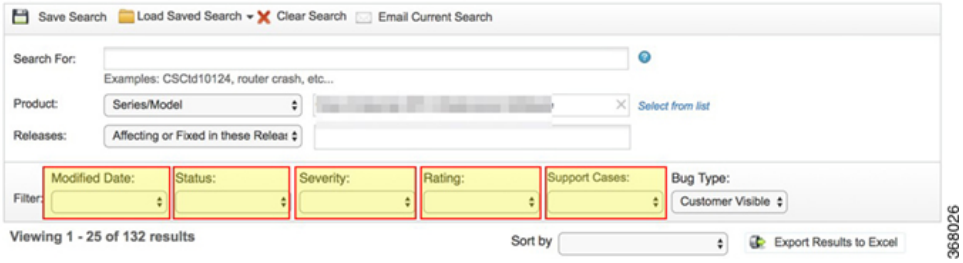
About the Cisco Bug Search Tool

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 Bengaluru 17.6.7

Identifier	Headline
CSCwh73350	Device keeps crashing when processing a firewall feature.
CSCwi14899	Device drops IPSEC traffic when SVI is used as source for DMVPN tunnel.
CSCwh99399	ftmd crashes in ENCS platform while running PWK suite.
CSCvo01546	NHRP reply processing may dequeue an unrelated request.
CSCwh49644	CSDL Compliance failure : Use of 3DES by IPSec is denied.
CSCwi01046	PoE module does not provide enough power to bring up the ports after an unexpected reload.
CSCwh01425	ITU channel configuration not working on device.
CSCwh20577	The TRACK client thread caused a crash due to an attempt to access an invalid memory location.
CSCwh70449	PMTUD is inaccurately converging without attempting to learn a higher MTU.
CSCwi59202	The C-NIM-2T module with SwitzerCC configuration is unable to start up in the IOS operating system.

Identifier	Headline
CSCwf34171	The 'configure replace' command is not working on IOS-XE devices because of an issue with the line 'license udi PID XXX SN:XXXX' in the configuration.
CSCwh36801	The system is experiencing a crash within the IP input process when performing tunnel encapsulation.

Open Caveats in Cisco IOS XE Bengaluru 17.6.7

There are no open bugs in this release.

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.6a

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 Bengaluru 17.6.6a

Identifier	Headline
CSCwe37016	The output rate on port channel does not match with the total physical interface output rate.
CSCwh14083	High CPU due to MPLS MIB poll.
CSCwf68612	Unexpected reload due to segmentation fault in WNCd process.
CSCwd16559	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table.
CSCwf99647	SRTP cipher failure for RTCP packets when AEAD_AES_256_GCM Cipher is used for call.
CSCwh21376	Unable to disable the call-home feature on devices.
CSCwb51779	Cisco IOS XE software privilege escalation vulnerability.
CSCwe93070	Tracebacks seen when configuring VRF with 32 characters or more.
CSCwf80400	IOS XE device may experience unexpected reset while executing the **show utd engine standard statistics** command.
CSCwd46688	Unable to apply the service policy on tunnel interface.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwe29301	AOM objects (FMAN_OBJ_ACL_REF) might be missing intermittently after MMA flapping.

Identifier	Headline
CSCwe90119	Device tracking database entry stuck on unknown state with temporal MAC address.
CSCwh15021	QFP crash when configuring S2S VPN (IKEv2/IPSEC).
CSCwf55145	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected.
CSCvu85539	Unable to delete wrong interface name.
CSCwd97212	UNIX-EXT-SIGNAL: Segmentation fault(11), Process = IOSXE-RP Punt service process.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwc67429	CTS PI changes for adding new binding source priority for LISP sourced local host bindings.
CSCwh45169	Unexpected reboot while dispalying information from cleared SSS session.
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site.
CSCwh49644	CSDL compliance failure : use of 3DES by IPSec is denied.
CSCwe91898	Environmental syslog is not appearing when power cord is disconnected from the redundant PS.
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCvz68895	The device crashed after adding trustpoint.
CSCvz32960	Device %IOSXE-3-PLATFORM: R0/0: /usr/sbin/pkg_to_tree: Failed to parse the key record 0. (28).
CSCwf95535	Intf/System xml files are not generated on the device.
CSCwf99947	Crash is seen when modifying tunnel after running the **show crypto** command.
CSCwd16419	Unexpected reload generates pubd core.
CSCwd97077	Device leaking memory because of telemetry subscription to collect FNF cache.
CSCwf78735	Device uses the NIM-1T/4T card for interconnection, and NAT+ GRE over IPSec cannot be applied.
CSCvy94747	Graceful Reload: Wrong state: 1 to receive chasfs event.
CSCwh12093	SOS/ROC feature on NIM.
CSCwh30377	Device data plane crash in umbrella/openDNS processing due to incorrect UDP length.
CSCwf34171	The **configure replace** command fails due to the license udi PID XXX SN:XXXX" line on IOS-XE devices.

Identifier	Headline
CSCwh45579	Unexpected reload on the device- ucode core @l2_dst_output_goto_output_feature_ext_path.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwf80191	Flowspec on the device will not revoke.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on the device.
CSCwf41084	Extranet multicast code improvements for better handling of data structure.
CSCwc87565	Unexpected reload due to a watchdog on the kernel.
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwd05362	Performance issue on device.
CSCwh36381	License feature HSECK9 not able to request on the device.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwe24491	Static NAT with HSRP stops working after removing / adding standby.
CSCwh42119	Ucode crash when ZBFW is configured on inside interfaces.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwf63706	HSRP received unexpected active hello packet when the interface recovered.
CSCwh01738	Unexpected reload when using rsh/rcmd.
CSCwf59929	CTS core process crash after configuring role based ACL.
CSCwh35397	Intermittent one way audio on RTP to SRTP calls with SSRC and sequence number changes.
CSCwe88689	ROMMON 17.6(6r) release for auto-upgrade.
CSCwh20577	Crashed by track client thread at access invalid memory location.
CSCwe21703	DMI for RESTCONF/NETCONF enters degraded state due to discriminator configured.
CSCvz20285	Device image information not updated in *packages.conf* when upgrading in autonomous mode.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup configuration.
CSCwf26494	BDI + NTP configuration puts DMI process in degraded mode.
CSCwd94495	SSM On-Prem responds with message *completed* to poll_id requests without ACK data.

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.6

Identifier	Headline
CSCwe09745	Memory leak in pubd when continuously trying to connect to remote peer.
CSCwd63063	Standby BGP session receives incorrect routes from active.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwd90168	Unexpected Reload after running the **show voice dsp** command while an ISDN call disconnects.
CSCwe98345	FHRP stay in active/active state after physical interface flap.
CSCwd45363	IPSec throughput level displays ambiguous outputs.
CSCwe24210	SNMP MIB does not show correct firmware version for the device.
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected.
CSCwb81159	Layer 2 RIB thread crashes when updating the MAC-IP.
CSCwe36122	ISIS crashes when performing TI-LFA calculation.
CSCwf03193	Device crashes with crash information files were generated with segmentation fault, process IPSec key engine.
CSCwf59173	Segmentation fault at IPv6 BGP backup route notification.
CSCwd88554	File system leak on standby device.
CSCwe20008	SNMP MIB OID changing its last index.
CSCwf00769	Layer 2 RIB thread crashes after removing EVPN member from bridge domain.
CSCwf39552	Segmentation fault by process mDNS on the device.
CSCwf83301	Cisco device displays incorrect values for call quality statistics (RTT/MOS).
CSCwe72462	Username/Password under voice register pool gets deleted post CME reload.
CSCwe25006	An unexpected removal of the underlay SG entry resulting ~20s disruption in the multicast flow SDA.
CSCwe21042	NBAR DP traceback - "Failed to process non-graph batch message: wrong batch id" is logged.
CSCwf47796	NHRP cache entries flood matching a /32 default route.
CSCwe32862	Router IOS-XE crash while executing AES crypto functions.
CSCwf09758	Watchdog crash while importing a large CRL file into the device.
CSCvy87339	Telemetry subscription fails to connect to GRPC receiver when multiple Xpath changes are made to it.

Identifier	Headline
CSCwe41946	DTMF is failing through IOS MTP during call on-hold.
CSCvq81894	Check next hop reachability before installing route for a prefix.
CSCwe52796	Intermittent one way audio issue after hold and resume. SRTP to RTP.
CSCvz12193	Authentication failure with MD5 SNMPv3 user.
CSCwd09685	Memory leak found @nfra/green/cep/src/cep.c.
CSCwe64213	LSPV if removal on OIF for RP discovery group 224.0.1.40 with timing related trigger.
CSCwf47563	Device is crashing after importing the trustpoint with RSA key pair.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwe33793	Memory allocation failure with extended antireplay enabled.
CSCwd59423	Unexpected reload on device caused by WNCd process after removing a VLAN from a VLAN-GROUP.
CSCwc03176	Device crashes when applying a service-policy to a newly created tunnel.
CSCwa96399	Configuring "entity-information" xpath filter causes syslogs to print, does not return data.
CSCwe70374	Device punt-policer is not configurable.
CSCwf41450	Device reloads changing the resource profile.
CSCwc24044	IOS XE device may experience an unexpected reset with high volume of multicast.
CSCwb47153	Keyman process crash.
CSCwc99453	Enable **license feature hseck9** command on the device.
CSCwd84391	Device incorrectly drops IP fragments due to reassembly timeout.
CSCwh05407	Gateway disconnecting incoming calls when FPI correlator is not released after disconnect on PRI leg.
CSCwb59052	Observe traceback message when BVM client do Inter-xTR roaming.
CSCwd73783	Observed qfp-ucode-wlc crash.
CSCwf14135	SIPREC recording fails in transfer scenario when certain options are enabled in configuration.
CSCwf56463	IOS process crash during VRRP hash table look up.
CSCwf44649	LISP failed to recreate the more specific away table entries after less specific entries toggled.
CSCwf48808	FlexVPN: Stale client routes stuck in RIB on FlexServer.

Identifier	Headline
CSCwf39490	MCID (Malicious Call Identification) gets broken due to custom prefix setting under STCAPP FAC.
CSCwa92418	Hide cisco-smart-*.yang from device by adding tailf:hidden full annotations.
CSCwd99921	IOS XE software crashes while validating certification trust.
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number.
CSCwc56033	Not triggering any alarms when RPM of a fan is 0.
CSCwf08019	TACACS+ authentication stops working after changing AES encryption key on the device.
CSCwe36743	Segmentation fault. SSH crashes when changing AAA group configurations.
CSCwf05980	Device dropping speed test/IPerf packets with drop reason drop-19 (IPv4NoRoute).
CSCwc97579	Spoke-spoke cache refresh not working correctly in case of multiple cache entries for same next hop.
CSCwh11858	Device running IOS-XE crashes when removing FQDN ACL.
CSCwc89823	Device crashes due to CPUHOG when walking ciscoFlashMIB @snmp_platform_get_flash_file_info.
CSCwf29859	Logging in get-config processing affecting the template push fail.
CSCwd28734	Device memory leak in pubd causes device reload.
CSCwf27815	DSP resource cannot be released after ending the call.
CSCuq20562	ISDN memory leak when PRI link flaps, crashes device.
CSCwf01986	Radius attribute 31 not being sent on the device for CTS PAC provisioning.
CSCwf03292	I/O middle pool leaking when VOIP trace is enabled.
CSCwe66318	NAT entries expire on standby device.
CSCwe60059	Device crashes when using dial-peer groups with STCAPP.
CSCwe39011	GARP on port up/up status from the router is not received by remote peer device.
CSCwf14589	IOS-XE device may experience a segmentation fault with Layer 2 VPN EVPN when clearing duplicate MAC.
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through the device.
CSCwh04884	VC down due to control-word negotiation.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit in the device.

Identifier	Headline
CSCwd49177	ISG: Layer 2 Connected Subscriber: IPv6 prefix delegation is not reachable when packet are switched.
CSCwf08698	Device crashes unexpectedly due to a fault in the 'TLSCLIENT_PROCESS'.
CSCwe18124	MACsec remains marked as secured, but randomly the traffic stops working.

Open Caveats in Cisco IOS XE Bengaluru 17.6.6

Identifier	Headline
CSCwe37016	The output rate on port channel does not match with the total physical interface output rate.
CSCwh14083	High CPU due to MPLS MIB poll.
CSCwf68612	Unexpected reload due to segmentation fault in WNCd process.
CSCwd16559	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table.
CSCwf99647	SRTP cipher failure for RTCP packets when AEAD_AES_256_GCM Cipher is used for call.
CSCwh21376	Unable to disable the call-home feature on devices.
CSCwb51779	Cisco IOS XE software privilege escalation vulnerability.
CSCwe93070	Tracebacks seen when configuring VRF with 32 characters or more.
CSCwf80400	IOS XE device may experience unexpected reset while executing the **show utd engine standard statistics** command.
CSCwd46688	Unable to apply the service policy on tunnel interface.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwe29301	AOM objects (FMAN_OBJ_ACL_REF) might be missing intermittently after MMA flapping.
CSCwe90119	Device tracking database entry stuck on unknown state with temporal MAC address.
CSCwh15021	QFP crash when configuring S2S VPN (IKEv2/IPSEC).
CSCwf55145	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected.
CSCvu85539	Unable to delete wrong interface name.
CSCwd97212	UNIX-EXT-SIGNAL: Segmentation fault(11), Process = IOSXE-RP Punt service process.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.

Identifier	Headline
CSCwc67429	CTS PI changes for adding new binding source priority for LISP sourced local host bindings.
CSCwh45169	Unexpected reboot while dispalying information from cleared SSS session.
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site.
CSCwh49644	CSDL compliance failure : use of 3DES by IPSec is denied.
CSCwe91898	Environmental syslog is not appearing when power cord is disconnected from the redundant PS.
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCvz68895	The device crashed after adding trustpoint.
CSCvz32960	Device %IOSXE-3-PLATFORM: R0/0: /usr/sbin/pkg_to_tree: Failed to parse the key record 0. (28).
CSCwf95535	Intf/System xml files are not generated on the device.
CSCwf99947	Crash is seen when modifying tunnel after running the **show crypto** command.
CSCwd16419	Unexpected reload generates pubd core.
CSCwd97077	Device leaking memory because of telemetry subscription to collect FNF cache.
CSCwf78735	Device uses the NIM-1T/4T card for interconnection, and NAT+ GRE over IPSec cannot be applied.
CSCvy94747	Graceful Reload: Wrong state: 1 to receive chasfs event.
CSCwh12093	SOS/ROC feature on NIM.
CSCwh30377	Device data plane crash in umbrella/openDNS processing due to incorrect UDP length.
CSCwf34171	The **configure replace** command fails due to the license udi PID XXX SN:XXXX" line on IOS-XE devices.
CSCwh45579	Unexpected reload on the device- ucode core @l2_dst_output_goto_output_feature_ext_path.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwf80191	Flowspec on the device will not revoke.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on the device.
CSCwf41084	Extranet multicast code improvements for better handling of data structure.
CSCwc87565	Unexpected reload due to a watchdog on the kernel.

Identifier	Headline
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwd05362	Performance issue on device.
CSCwh36381	License feature HSECK9 not able to request on the device.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwe24491	Static NAT with HSRP stops working after removing / adding standby.
CSCwh42119	Ucode crash when ZBFW is configured on inside interfaces.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwf63706	HSRP received unexpected active hello packet when the interface recovered.
CSCwh01738	Unexpected reload when using rsh/rcmd.
CSCwf59929	CTS core process crash after configuring role based ACL.
CSCwh35397	Intermittent one way audio on RTP to SRTP calls with SSRC and sequence number changes.
CSCwe88689	ROMMON 17.6(6r) release for auto-upgrade.
CSCwh20577	Crashed by track client thread at access invalid memory location.
CSCwe21703	DMI for RESTCONF/NETCONF enters degraded state due to discriminator configured.
CSCvz20285	Device image information not updated in *packages.conf* when upgrading in autonomous mode.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup configuration.
CSCwf26494	BDI + NTP configuration puts DMI process in degraded mode.
CSCwd94495	SSM On-Prem responds with message *completed* to poll_id requests without ACK data.

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.5a

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 Bengaluru 17.6.5a

Identifier	Headline
CSCvy23366	Device + UCSE: Kernel crash on the device with UCSE module.
CSCwd79089	Device controller crashes 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.
CSCwd45363	Device IPSEC throughput level is ambiguous outputs.
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 not sending properly NBAR application information.
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client.
CSCwc56033	Not triggering any alarms when RPM of a fan is 0
CSCwd49177	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packet are switched.

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.5

Identifier	Headline
CSCvz93612	The message %HW_FLOWDB-3-HW_FLOWDB_DBLDEL_FEATOBJ: FlowDB featobj cannot be deleted twice.
CSCvy60839	CSDL Compliance: Add CLI to disable CSDL compliance.
CSCwc82140	QFP crashes when ZBFW configuration features "log dropped-packets" configuration.
CSCwc99823	The FMAN crash is seen in SGACL@ fman_sgacl_calloc.
CSCvz92994	Lack of MAC address in Inform Event message.
CSCwb52324	Device unexpected reload due to QFP ucode crash.
CSCwd71584	DSPware 58.5.2 release targeting v176_throttle.
CSCwd61255	Data Plane Crash is seen on the device when making Per-Tunnel QoS configuration changes with scale.
CSCwb04815	NHRP process taking more CPU because of FlexVPN event trace.
CSCwc22314	RTSP traffic not being rewritten by NAT.

Identifier	Headline
CSCwc28587	Device crashed without generating any core (Critical process plogd fault on rp_0_0 (rc=75).
CSCwd72312	GETVPN- Traffic drops seen on GM after rekey installing policies on the image.
CSCwd30578	Wired guest client stuck at IP_LEARN with dhcp packets not forwarded out of the foreign to anchor.
CSCwb73395	Need CLI option to disable ALG.
CSCwc54463	Devie module is down when high CPU noticed.
CSCwc72923	ERROR info: Router configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt.
CSCwc84967	Intermittent double DTMF due to changing timestamp on a DTMF event.
CSCwb08057	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
CSCwd47123	ISG uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply.
CSCwb32635	File is incomplete when running admin-tech.
CSCwd33202	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface.
CSCwh01936	Secure calls with GCM cipher fail.

Open Caveats in Cisco IOS XE Bengaluru 17.6.5

Identifier	Headline
CSCvy23366	Device + UCSE: Kernel crash on the device with UCSE module.
CSCwd79089	Device controller crashes 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.
CSCwd45363	Device IPSEC throughput level is ambiguous outputs.
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 not sending properly NBAR application information.
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client.
CSCwc56033	Not triggering any alarms when RPM of a fan is 0

Identifier	Headline
CSCwd49177	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packet are switched.

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.4

Identifier	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 Expereincing IOS Tracebacks, followed by KEYMAN crashes.
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
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 is seen with umbrella config during soak run.
CSCvz83016	BFD tunnel uptime not showing 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.
CSCwb90470	Device crashed with last reload reason Critical process cxpd fault.
CSCwb73511	Device is not able to bring up SIG tunnels after reboot.
CSCwb91729	Fix mishandling of policy sequence programming failures and notify with syslog/notification.
CSCwa67886	UDP based DNS resolution doesn't work with IS-IS EMCP on IOX-XE.
CSCwb85046	Device reloads when group-range is configured under an interface Group-Async.
CSCwc39881	CSR generated from hardware cEdge contains "/" in common name.
CSCvz23982	IOS sending UP Event for the sub interface which is in down state.
CSCvx93283	Service Chain is not created when Tracking is disabled.
CSCvx18302	[SIT] Speed Test to Internet failing on cEdges running 17.3.
CSCvz99832	cEdges per class BFD - echo response pakets.
CSCwb08636	IPSEC-3-HMAC_ERROR: IPSec SA receives HMAC error seen for TLOCExt setup after upgrade.

Identifier	Headline
CSCvx74917	DNS Packets are not redirected to configured Custom DNS after Umbrella Template Edit.
CSCwb73664	Show sdwan bfd session" have missing last digit for site-id.
CSCwa72273	ZBFW dropping return packets from Zscalar tunnel post cEdges upgrade to 17.3.4.
CSCwa64955	cEdge loses control connections after installing new enterprise hardware wan edge certificate.
CSCwa92137	cEdge is changing ICMP ID in ICMP echo replies intermittently.
CSCwa49721	HUB with firewall configured incorrectly dropping return packets when routing between VRFs.
CSCwa81471	AOM pending objects with loopbacks binded to tloc-extended interfaces.
CSCwb49857	Memory leaks on keyman process when key is not found.
CSCwb76866	CSDL failure: Use of MD5 by IPSEC key engine is denied.
CSCwb16723	Traceroute not working on cEdge with NAT.
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored.
CSCwc13304	Per-tunnel QoS counters and shapers not working for some bfd tunnel with stale 'nh_overlay' objects.
CSCwa67398	NAT translations do not work for FTP traffic in the device.
CSCwb78173	CSDL failure: IPSec QM Use of DES by encrypt proc is denied.
CSCwb71658	Traceback seen on C8300-2N2S-4T2X after enabling ipsec_pwk and reboot.
CSCwb76170	zScalaer IPsec SIG auto tunnels are not coming up.
CSCwb41907	CPP uCode crash due to ipc congestion from dp to cp.
CSCwb74917	Device incorrectly drops ip fragments due to reassembly timeout.
CSCvy54048	CPP Unexpected Reboot While Freeing CVLA Chunk
CSCwa30857	Internet SpeedTest with Loopback binding mode doesn't work with implicit ACL drop for return traffic
CSCwb14020	Serial interface stuck in "line protocol is down" state after it went down and it is recovered.
CSCwa98545	Checks of route leaks creates memory corruption.
CSCwb46649	NAT translation don’t show (or use) correct timeout value for an established TCP session.
CSCwa08847	ZBFW policy stops working after modifying the zone pair.

Identifier	Headline
CSCwc33311	cEdge crashes @ imgr_n2_ipsec_sa_ctx_register.
CSCwa26599	FN980 new signed Telit modem firmware FN980M_38.02.X92 upgrade failed.
CSCwb12647	Device crashes for stuck threads in cpp on packet processing.
CSCwc04688	cEdge crash observed after enabling NWPI trace with IPv6 traffic.
CSCwb78290	CISCO-SDWAN-BFD-MIB request gives results intermittently.
CSCwb76988	IKEv2 fragmentation causes wrong message ID used for EAP authentication.
CSCvw50622	NHRP network resolution not working with link-local ipv6 address.
CSCwb59736	CSR BFD tunnel are zero with SDWAN version 17.03.03.0.7.
CSCwa57873	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request.
CSCvz37340	The [service timestamps log datetime msec localtime] command cannot be pushed via CLI Addon template
CSCwb99793	CRL verification failure result 400 Bad Request with DigiCert.
CSCwa25256	Installing new enterprise wan edge cert does not remove old cert causing device to use old certificate.
CSCwb51595	Missing IOS config (voice translation rule) on upgrade from 17.3 to 17.6.
CSCwb40575	After cedge upgrade, umbrella dns config set to NONE in show umbrella config (17.4.2 to 17.6.3).
CSCwb18315	Umbrella DNS security policy doesn't work with Cloud onRamp with SIG tunnels.
CSCwb58468	17.8 Sig Autotunnels:tunnel 409 response received.
CSCwc04289	cEdge: Inconsistency between Path MTU Discovery result and Tunnel MTU.

Open Caveats in Cisco IOS XE Bengaluru 17.6.4

Identifier	Headline
CSCwc62269	CG522-E: vDaemon process may fail to start, vManage control connection may fail as DCONFAIL
CSCwd36511	Ping fail to VRRP virtual IP address.
CSCwb62474	Device may crash when doing SDWAN speedtest with WAN flapping.
CSCwc23077	Firewall drop seen stating “FirewallL4” seen on the device.
CSCwb74821	Yang-management process confd is not running in controller mode 17.6.2a.
CSCvz92994	Lack of MAC address in Inform Event message.

Identifier	Headline
CSCwc50477	Devicecrashed in ipv4_nat_create_out2in_session_entry.
CSCwc55260	Memory leak due to FTMd process.
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site.
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCwb90375	Adding Modem to AUX port results in having to Toggle Modem InOut or Reload the Router.
CSCwc59598	Statistics collection causing service-side BFD to flap on every collection interval.
CSCwc52538	Flows are not distributed and load-balanced evenly and consistently.
CSCwb83236	Traceback: QFP core after pushing data policy with IPv6 interface.
CSCwc67465	tDevice cannot be upgraded to 17.8.
CSCwc59650	Show sdwan app-fwd cflowd flows vpn X format tabled does not show all flows for vpn X.
CSCwc25291	NIM-LTE-EA No Data - Requires subslot reload to recover.
CSCwc63563	Unable to set specific speed and duplex values on SFP ports on IOS-XE routing platforms.
CSCwc43973	DLC is not completing after upgrading to Smart licensing from CSL.
CSCwc53885	IOS-XE "no ip nat" config is allowed to be committed and removes nat routes among other nat configurtation.
CSCwc63337	Destination not reachable if configured as a next for a static route resolvable via non /32 OMP.
CSCwc30050	UTD: Exception in utd_logger.py due to missing extra-data in AMP alert.
CSCwc27208	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES.

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.3a

Identifier	Headline
CSCvy63924	Telemetry: IOS-XE Controller crashes after using 'show telemetry ietf subscription all' command.
CSCvx40516	ZBFW + NAT: Traffic flow In2Out scenario failed
CSCwa26509	Shut/no shut of endpoint-tracker attached tunnel, does not create probe again on 17.6.2.
CSCvz98373	ZBFW: FirewallPolicy drops seen with RTSP traffic in steady state.

Identifier	Headline
CSCvz99404	SD-WANImplicitAclDrop seen on non-SDWAN interface after upgrade to 17.6.1
CSCvz71436	Call Placing issue from SCCP phones.
CSCvy69846	Guestshell:.py files stored under /home/guestshell are lost after reboot on 1ng device.
CSCwa38451	Packets loss happens on C8300 when inserting SFP into or no shut other IF with a SFP.
CSCvy57681	Unexpected reboot of IOS-XE Router in BQS QM @ cpp_qm_proc_rt_commit.
CSCvz86591	VRF-aware static NAT with route-map and reversible not working.
CSCwa30988	CoS preservation not working for the services EVPL and EPL tunnel.
CSCwa36699	Prefetch CRL Download Fails.
CSCvz62032	Attach gateways failed in cloud express.
CSCwa19074	Infinite output from command show sdwan tunnel sla
CSCwa80474	IKEv2 Deprecated Ciphers denied by Crypto Engine CDSL - Cicso PSB Security Compliance.
CSCvv82985	dhcpv6_relay:dhcp-client on branch not receive ipv6 address
CSCwa76260	IKEv2 Deprecated Ciphers denied by Crypto Engine CDSL - Cicso PSB Security Compliance
CSCvt66541	Crypto PKI-CRL-IO process crash when PKI trustpoint is being deleted.
CSCwa11150	E1 configurations (under Serial interface) lost after reload.
CSCvz65545	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535.
CSCvz41647	Partial multicast drops are seen after a failover event in a site with two cedges.
CSCvz76277	Hostname not allowed beginning with numbers.
CSCvz34668	Static mapping for the hub lost on one of the spokes.
CSCwa15085	Router Crash due to Stuck Thread with appnav-xe dual controller mode.
CSCvx28426	Router may crash due to Crypto IKMP process.
CSCwa18177	Flapping bidirectional/unidirectional packet capture option with ipv4 filter for long time failed.

Open Caveats in Cisco IOS XE Bengaluru 17.6.3a

Identifier	Headline
CSCvz93712	VFR is enabled by feature NAT but there is no NAT configured on the interface
CSCvy72970	Active ftp not working with UTD+HTX for security and Unified policy.
CSCwa39336	CG522: Cannot transfer files.
CSCwa57254	Silent Reload due to CpuCatastrophicError.
CSCwb20089	cEdge ESP crashes after enable platform debug for Cloud onRamp for SaaS.
CSCvx74917	DNS Packets are not redirected to configured Custom DNS after Umbrella Template Edit
CSCwb03662	CDP/LLDP not working when 10GE interface enabled with MACSEC.
CSCwb00533	cEdge traffic is getting dropped/blackholed due to OCE_ADJ_DROP reason.
CSCwb25913	After configuring match input-interface on class-map, router goes into a reboot loop
CSCwb03455	Inter-vrf route leaking not working and packet drop seen due to Ipv4Unclassified
CSCwa72273	ZBFW dropping return packets from Zscalar tunnel post cEdge upgrade to 17.3.4.
CSCwa68471	Traceback: CPP ucode core generated after HSRP priority change.
CSCwa49721	Cisco SD-WAN HUB with firewall configured incorrectly dropping return packets when routing between VRFs.
CSCwb18223	SNMP v2 community name encryption problem.
CSCwb08186	E1 R2 - dnis-digits cli not working
CSCwa81471	AOM pending objects with loopbacks binded to tloc-extended interfaces.
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes.
CSCvy54048	CPP Unexpected Reboot While Freeing CVLA Chunk.
CSCwa98545	Checks of route leaks creates memory corruption.
CSCvz08674	cEdge rebooted 2 time with CPP 0 failure Stuck Thread.
CSCwa76875	After configuring match input-interface on class-map, router goes into a reboot loop.
CSCwa08847	ZBFW policy stops working after modifying the zone pair.
CSCwa26599	New signed Telit modem firmware FN980M_38.02.X92 upgrade failed.
CSCwa29964	SCEP fails if AAAA DNS repy is received and source interface has no IPv6 address.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions.
CSCvz55275	Show DMVPN command displays incorrect state.

Identifier	Headline
CSCwa74499	ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection.
CSCwb18315	Umbrella DNS security policy doesn't work with Cloud onRamp.

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.2

Caveat ID Number	Description
CSCvy37285	SSH to Loopback not working.
CSCvy44723	Control connection to the edege device doesnt come up with v6 and reverse proxy.
CSCvy54606	CVLA need to reserve at least 50M memory for low-end DRAM platform.
CSCvy74799	Ucode crash observed at tw_bad_timer_bucket () at ../../../infra/tw_timer.c:918.
CSCvy74977	Catalyst 8300 flooded with Tx Unit Hang messages.
CSCvy85281	Crash triggered by "crypto gdoi ks rekey replace-now".
CSCvy89362	QOS-3-INVALID_BQS_QUEUE_INFO: Drop policy given an invalid scheduling queue/wred 0/0 -Traceback.
CSCvy89461	Crash when getting cdspCardStatusEntry OID.
CSCvy89785	OSPFv3 adjacency does not come up after "ospfv3 authentication ipsec" is applied on Tunnel interface.
CSCvy92960	QFP FirewallNonsession drops when starting 80K flows.
CSCvy94954	LA LED turns green when just inserted SFP-10G-LR on the device without cable connecting.
CSCvy95586	SCCP gateway auto configuration download results in an incomplete configuration.
CSCvy97578	Need Active/Active ZBFW support for Inter-vrf TCP traffic.
CSCvy97761	IPV6 route is breaking control connection.
CSCvy98784	AppQoE DP stats for active connections shows huge bogus value.
CSCvz00054	Catalyst 8300 nested IPSec tunnels encryption does not work as expected.
CSCvz03053	OMP continues to redistribute BGP route with down bit set (SoO).
CSCvz03342	Multicast boundary command on tunnel interface DMVPN network is sending ttl=1 packet.
CSCvz07134	Router does not boot on recent 16.X releases with large service policy applied on the interface.
CSCvz07542	Device with NIM-ES2 "no igmp snooping vlan x" is not preserved after reload.

Caveat ID Number	Description
CSCvz08449	Incorrect static route for primary interface during deployment resulting in unreachability.
CSCvz09078	FireWall Policy Drops are seen when the OG/ACE's are reconfigured multiple times.
CSCvz09330	Bootstrap aaa config issues due to default aaa configuration.
CSCvz18867	IP NAT source static does not work for TCP traffic from OUT to IN.
CSCvz20181	C8500L: Overruns happening when flow-control enabled.
CSCvz23024	17.6.1_auto:SNMP failure on bfdSessionsListSystemIp
CSCvz24267	Static NAT entry is injecting a route to Null0.
CSCvz26211	Flow monitor statistics missing when reloading with configuration.
CSCvz30465	MT: Template push with thousand eye feature failed on the device after PnP workflow.
CSCvz34290	no ip nbar resources flow max-session does not restore default platform session limits
CSCvz35812	Cpp_cp_svr crash in ZBF component.
CSCvz45256	Inbound fax T38 switchover on MGCP GW sending an m line of audio instead of image.
CSCvz47421	VLAN IP config missing on bootup due to missing startup configs.
CSCvz47982	Flow-Control Goes down when configurating manual speed and remove the auto negotiation.
CSCvz53819	ZBFW: ARStandby drops seen on New Active during RG switchover.
CSCvz55789	Data-policy direction-all with empty action is causing to ignore app-route-policy.
CSCvz56966	Zscaler SIG tunnels not coming up after reboot due to HTTP/RESP/CODE 400.
CSCvz60101	Failure to start (on RP2) iox app-hosting application.
CSCvz62602	Extranet local switch crash when mdata is enabled.
CSCvz69124	BFD scaling: Not able to scale more that 2048 BFD sessions.

Open Caveats in Cisco IOS XE Bengaluru 17.6.2

Caveat ID Number	Description
CSCvv82985	dhcpv6_relay:dhcp-client on branch not receive ipv6 address.
CSCvw67366	Punt keepalive crashed due to bqs related interrupt.
CSCvx28426	Router may crash due to Crypto IKMP process.
CSCvy57681	Unexpected reboot of IOS-XE Router in BQS QM @ cpp_qm_proc_rt_commit.

Caveat ID Number	Description
CSCvy63924	Telemetry: IOS-XE Controller crashes after using show telemetry ietf subscription all command.
CSCvy69846	Guestshell:.py files stored under /home/guestshell are lost after reboot on 1ng device
CSCvy72970	Active ftp not working with UTD+HTX for security and Unified policy.
CSCvz11362	Device fails to install rekey causing traffic drop.
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes.
CSCvz31901	ASR1K: Cisco makefile changes to build the PHY API SW 4.67.05
CSCvz37340	The **service timestamps log datetime msec localtime** command cannot be pushed via CLI Addon template.
CSCvz40459	Ucode crash due to NAT proxy timeout.
CSCvz50890	Memory leak at FTMD SDWAN running 17.03.02
CSCvz54262	Device crashes at CFT after scaling up to 4M flows when internet link up from 2Gbps to 10Gbps.
CSCvz55812	MLP cpp crash cause both FP cpp to lock and stuck in disconnecting.
CSCvz58895	IOS-XE unable to export elliptic curve key.
CSCvz65545	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535.
CSCvz74322	The **Shutdown** command visible in running config after reload of ASR 1002-HX
CSCvz76277	Hostname not allowed beginning with numbers.
CSCvz80197	FTMD message error
CSCvz84437	Unexpected reload due IPV6 UDP fragment header in VxLAN

Resolved Caveats in Cisco IOS XE Bengaluru 17.6.1a

Caveat ID Number	Description
CSCvo41609	GETVPN: Clearing members on Key Server causing rekey processing failure on GMs.
CSCvq11402	[SSL-Proxy-Policy] Webroot - url cloud lookup timeout is 60s (way too long to hold the traffic).
CSCvw91361	Crash when issuing "show crypto isakmp peers config".
CSCvx25217	Issue with removing the NAT configuration from the template in a single operation if NAT translation is active.
CSCvx32670	Wrong reload reason reflected after a power outage.

Caveat ID Number	Description
CSCvx53399	Fman_fp_image crashed with ZBFW config change.
CSCvx57615	ZBFW blocking ACK packets for applications using cloudexpress SaaS set to use a Gateway with synsent.
CSCvx64449	%CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: mac verify failed due to ip rtp header-compression iphc-format
CSCvx64640	Data plane VPLS traffic generating Control Word on all Label Switched Headers
CSCvx68767	PWK - Overlay tunnel goes down with overnight traffic (No Crash)
CSCvx72682	[DMM/SLM test issue] CFM crash when using physical port, DMM/SLM doesn't work on EVC.
CSCvx77024	IPv6 DMVPN - NBMA address not getting preserved
CSCvx77203	Router crashed when sending traffic through non-SDWAN interface with DIA NAT + debug enabled.
CSCvx77674	A router may crash when processing an NHRP packet.
CSCvx78215	An IOS XE device might crash at DoubleExceptionVector.
CSCvx83301	Insufficient resources" NHRP-ERROR while receiving small rate of NHRP Resolution Requests/second.
CSCvx85334	Port enters err-disabled state (BPDU guard) when LLDP packet with MAC DA:0180.c200.0000.
CSCvx88246	Packets dropped due to firewall + data policy interop issue.
CSCvx89710	SCEP: CA server fails to rollover CA certificate with error: "Storage not accessible"
CSCvx94323	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut
CSCvx97718	VTCP frees rx buffer when packet with expected next sequence arrives with no payload; phones reset.
CSCvy01097	Router may crash under ZBF configuration (cpp_cp_svr)
CSCvy10159	Software MTP should support encrypted TLS connection
CSCvy13735	BFD tunnels stuck in down state after port-hop
CSCvy18284	Poor IPsec throughput performance with IPsec throughput license on IOS-XE routers
CSCvy20588	CSDL failure when it should be allowing RSA keys with 1024 length.
CSCvy30209	IOS-XE cpp ucode crash with fragmented packets.
CSCvy32935	UTD: Pickup latest SPPI library with fix for CSCvy00963
CSCvy33007	"Best of Worst" Fallback mode causes reachability issue when routes flap.

Caveat ID Number	Description
CSCvy33818	On MTT vManage system IP persists after invalidating and deleting the edge devices.
CSCvy34102	CPP ucode crash with route-map and overload at ipv4_nat_rmap_walk_find.
CSCvy35044	Signature update failure - SSL-CERTIFICATE_VERIFY_FAILED.
CSCvy52761	Adding multilink frame relay sub-interface to SDWAN fails; "Aborted: application error".
CSCvy54314	Data-policy local-tloc with app-route is dropping packets when SLA is not met.
CSCvy67301	URL Filtering regex pattern match not working on large pattern
CSCvy93830	BFD tunnel uptime not showing correct values post upgrade to 17.6.01

Open Caveats in Cisco IOS XE Bengaluru 17.6.1a

Caveat ID Number	Description
CSCvy33818	On MTT vManage system IP persists after invalidating and deleting the edge devices.
CSCvy72970	Active ftp not working with UTD+HTX for security and Unified policy.
CSCvy78501	17.6: AAR not working properly as configured SLA classes are not shown under app-route stats
CSCvy86497	BFD session flap/down while control connection with vManage is going down
CSCvy87507	Router unexpectedly routes traffic with broadcast dst MAC
CSCvy98784	AppQoE DP stats for active connections shows huge bogus value
CSCvz06095	ReassTimeout drops with NAT in Port-Channel.
CSCvz08674	cedge rebooted 2 time with CPP 0 failure Stuck Thread
CSCvz08945	low-bandwidth-link doesn't reduce number of BFD packets
CSCvz09078	FireWall Policy Drops are seen when the OG/ACE's are reconfigured multiple times
CSCvz25403	NetApp: Issues with traffic does not get forwarded via TLOC extended interface
CSCvz28795	SSL VPN fails to establish if 'match url' is configured under crypto ssl profile
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes
CSCvz33108	After uploading the serial file list to the vmanage, the edges lost Control Con. and BFD sessions
CSCvz35990	OSPFv3 IPSec encryption failure when IPv4 address-family not configured in VRF
CSCvz40788	SDWAN tunnels are not coming up in Multilink Frame relay sub-interface.
CSCvw50713	Restore NBAR FIA on VPG interface.

Related Documentation

- Hardware Installation Guide for Catalyst 8200 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8300 Series Edge Platforms
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Cisco Catalyst 8300 and 8200 Series Edge Platforms Software Configuration Guide

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.