Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Cisco IOS XE Bengaluru 17.6.x

First Published: 2021-07-29

Last Modified: 2024-04-04

Full Cisco Trademarks with Software License

About Cisco Catalyst 8500 Series Edge Platforms

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Note Cisco IOS XE Bengaluru 17.6.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE Bengaluru 17.6.x release series.

The Cisco Catalyst 8500 Series Edge Platforms are high-performance cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

The Cisco Catalyst 8500 Series Edge Platforms includes the following models:

- C8500-12X4QC
- C8500-12X
- C8500L-8S4X

For more information on the features and specifications of Cisco 8500 Series Catalyst Edge Platform, refer the Cisco 8500 Series Catalyst Edge Platform datasheet.

Sections in this documentation apply to all models of unless a reference to a specific model is made explicitly.

Note Starting with Cisco IOS XE Amsterdam 17.3.2 release, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

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

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

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.

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the features, platform, and software image support on Cisco Catalyst 8500 Series Edge Platforms. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/ An account on cisco.com is not required.

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 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.

Table 1: Software Features

Feature	Description
L2VPN Traffic SteeringUsing 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.

Open and Resolved Bugs for Cisco IOS XE Bengaluru 17.6.7

Resolved Bugs for Cisco IOS XE Bengaluru 17.6.7

Identifier	Headline
CSCwh73350	Device keeps crashing when processing a firewall feature.
CSCwi59202	The C-NIM-2T module with SwitzerCC configuration is unable to start up in the IOS operating system.
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.

Identifier	Headline
CSCwf62757	Issue with the frequency of data reporting for the physical device interface.
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 Bugs for Cisco IOS XE Bengaluru 17.6.7

There are no open bugs in this release.

Open and Resolved Bugs for Cisco IOS XE Bengaluru 17.6.6a

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool , each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Resolved Bugs for Cisco IOS XE Bengaluru 17.6.6a

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 Bugs for 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
CSCwh12093	SOS/ROC Feature on NIM
CSCwh14083	ASR1k- High CPU due to MPLS MIB poll
CSCwf68612	9800 WLC 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 SDWAN devices
CSCwf34171	"Configure replace" command fails due to the "license udi PID XXX SN:XXXX" line on IOS-XE devices
CSCwb51779	Cisco IOS XE Software Privilege Escalation Vulnerability
CSCwe93070	Tracebacks seen when configuring VRF with 32 characters or more
CSCwf80400	IOS XE Router may Experience Unexpected Reset while executing 'show utd engine standard statistics'
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) with Azure vWAN/HUB
CSCwf55145	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected
CSCvu85539	SDWAN, CSR1Kv: unable to delete wrong interface name

Identifier	Headline
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	ISR4K: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/pkg_to_tree: Failed to parse the key record 0. (28)
CSCwh42119	Ucode crash when ZBFW is configured on inside interfaces
CSCwf95535	Intf/System xml files are not generated on cEdge
CSCwf99947	Crash when modifying tunnel after running "show crypto" commands
CSCwd16419	C9800-CL-K9 unexpected reload generates pubd core
CSCwd97077	ISR leaking memory in MallocLite because of telemetry subscription to collect FNF cache
CSCwf78735	C8200 uses the NIM-1T/4T card for interconnection, and NAT+ GRE over ipsec cannot be applied
CSCvy94747	GRACEFUL-RELOAD: Wrong state: 1 to recieve chasfs event:
CSCwe37123	8500 Uses Excessive Memory When Configuring ACLs with Large Object Groups
CSCwh30377	ASR1K data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length
CSCwd90056	C8500-12X4QC P2MP WAN MACSEC does not allow traffic to pass on the link
CSCwh45579	Unexpected reload on ASR1k 17.3.5 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

Identifier	Headline
CSCwf80191	flowspec on ASR1k won't revoke
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on C1117-4PLTEEA
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 ASR1k to crash
CSCwd05362	Performance issue on ASR900 platform
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted
CSCwe24491	ISR4k : Static NAT with HSRP stops working after removing / adding standby
CSCwf62757	C8500L Interface data report interval issue for physical interface
CSCwf71557	IPv4 connectivity over PPP not restored after reload
CSCwh01738	Unexpected reload when using rsh/rcmd on 17.6
CSCwf59929	CTS CORE process crash after configuring role based ACL
CSCwh35397	Intermittent one way audio on RTP to SRTP calls with SSRC and seq num changes
CSCwh20577	Crashed by TRACK Client thread at access invalid memory location
CSCwe21703	DMI for RESTCONF/NETCONF Enters Degraded State due to Discriminator Configured
CSCvz20285	SDWAN image info not updated in packages.conf when upgrading in autonomous mode
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config
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

Open and Resolved Bugs for Cisco IOS XE Bengaluru 17.6.6

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool , each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Resolved Bugs for 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 **show voice dsp** command while an ISDN Call Disconnects
CSCwe60059	Crash when using dial-peer groups with STCAPP
CSCwe28204	C8500L : Control connection over L3 Tloc extension failing as no NAT table entry created
CSCwe24210	SNMP MIB does not show correct firmware version for LTE module
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected
CSCwb81159	L2RIB thread crash when updating the MAC-IP
CSCwe36122	ISIS crash when performing TI-LFA calculation
CSCwf03193	Device crash with crashinfo files were generated with Segmentation fault, process IPSEC key engine
CSCwf59173	Segmentation fault at IPv6 bgp backup route notification

Identifier	Headline
CSCwe10905	Device tracker
CSCwd88554	Filesystem leak on standby device
CSCwe20008	Device SNMP MIB OID changing its last index
CSCwf00769	L2RIB thread crash after removing EVPN member from bridge domain
CSCwf39552	Segmentation fault by process on device
CSCwf83301	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 S,G 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	Device IOS-XE crash while executing AES crypto functions
CSCwf09758	Watchdog crash while importing a large CRL file into switch.
CSCwf67564	Device observes Memory Leak at process SSS Manager
CSCvy87339	Telemetry Subscription fails to connect to GRPC receiver when multiple XPATH changes are made to it.
CSCwe41946	DTMF is failing through IOS MTP during call on-hold
CSCvq81894	Check nexthop reachability before installing route for a prefix
CSCwc20170	Device reloads unexpectedly due to critical FTMd fault when VRF Configuration is pCSCwe24491ushed
CSCvz12193	snmpwalk: Authentication failure, with MD5 SNMPv3 user
CSCwd09685	Memory leak found @nfra/green/cep/src/cep.c
CSCwe64213	[SDWAN-Autorp]: LSPVif removal on OIF for RP discovery group 224.0.1.40 with timing related trigger
CSCwf47563	Device is crashing after importing the trustpoint with rsakeypair
CSCwe12194	Auto-Update Cycle incorrectly deletes certificates
CSCwe33793	Memory allocation failure with extended antireplay enabled
CSCwd59423	Unexpected Reload on C9800 Caused by WNCd Process After Removing a VLAN from a VLAN-GROUP

Identifier	Headline
CSCwc03176	ASR1K 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
CSCwh04884	ASR903:17.6.3: VC Down due to control-word negotiation
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 8200L platform
CSCwb59052	Observe Traceback message when BVM client do Inter-xTR roaming
CSCwd73783	17.3.6 - 9800-L - Observed qfp-ucode-wlc crash
CSCwf14135	SIPREC recording fails in transfer scenario when certian options are enabled in configuration
CSCwf56463	IOS process crash during VRRP hash table lookup
CSCwf44649	LISP failed to recreate the more specific away table entries after less specific entries toggled.
CSCwe23150	CUBE memory leak sdp_copy_all_attrs sdp_parse_attribute sdp_add_new_attr
CSCwf48808	FlexVPN: Stale Client Routes Stuck in RIB on FlexServer
CSCwf39490	MCID (Malicious Call Identification) gets broken due to Custom prefix setting under STCAPP FAC
CSCwa92418	hide cisco-smart-*.yang from SDWAN device by adding tailf:hidden fullâ annotations
CSCwd99921	IOS XE software crash while validating certification trust
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M)
CSCwe69783	VG420 can lose its config during a triggered resync process if lines are in an off-hook state
CSCwc56033	Not triggering any alarms when RPM of a fan is 0
CSCwf08019	TACACS+ authentication stops working after changing AES encryption key on the WLC
CSCwe36743	Segmentation Fault - Crash - SSH - When Changing AAA Group Configs
CSCwe52796	Intermittent one way audio issue after hold and resume. SRTP to RTP
CSCwe41234	VG450 VMWI Race Condition Causes No Ringing for Analog Phones

Identifier	Headline
CSCwf55830	VG450/VG3x0 No Dial Tone on Analog Phones due to DSP going into Power Denial State
CSCwc97579	Spoke-spoke cache refresh not working correctly in case of multiple cache entries for same next hop.
CSCwf41082	MallocLite Memory Leak observed in HTTP CORE Allocator
CSCwh11858	Switch running IOS-XE crashes when removing FQDN ACL
CSCwc89823	Router 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	Cat9k memory leak in pubd causes switch reload
CSCwf27815	DSP resource can not be release after end the call
CSCuq20562	ISDN Memory Leak when PRI link flaps, crashes Router
CSCwf01986	Radius attribute 31 not being sent on 9300 for CTS Pac provisioning
CSCwf03292	I/O middle pool leaking when VOIP trace is enabled
CSCwe66318	NAT entries expire on Standby Router
CSCwh05407	Gateway disconnecting incoming calls when FPI Correlator is not released after disconnect on PRI Leg
CSCwe39011	GARP on port up/up status from C8300 router is not received by remote peer device.
CSCwf14589	IOS-XE Switch May Experience a Segmentation Fault with L2VPN EVPN When Clearing duplicate MAC
CSCwe70237	Cube reloads due to a segmentation fault in CCSIP_SPI_CONTROL process
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through Router
CSCwf24164	Netflow stops working when flow monitor reaches cache limit in 8500L
CSCwd49177	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packet are switched
CSCwf08698	Cat9k Crashes Unexpectedly due to a Fault in the 'TLSCLIENT_PROCESS'
CSCwe18124	MACsec remains marked as Secured, but randomly the traffic stops working
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M)

Open Bugs for 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
CSCwh12093	SOS/ROC Feature on NIM
CSCwh14083	ASR1k- High CPU due to MPLS MIB poll
CSCwf68612	9800 WLC 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 SDWAN devices
CSCwf34171	"Configure replace" command fails due to the "license udi PID XXX SN:XXXX" line on IOS-XE devices
CSCwb51779	Cisco IOS XE Software Privilege Escalation Vulnerability
CSCwe93070	Tracebacks seen when configuring VRF with 32 characters or more
CSCwf80400	IOS XE Router may Experience Unexpected Reset while executing 'show utd engine standard statistics'
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) with Azure vWAN/HUB
CSCwf55145	SFP transceiver DOM not working after some time, however interface forwards the traffic as expected
CSCvu85539	SDWAN, CSR1Kv: 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

Identifier	Headline
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	ISR4K: %IOSXE-3-PLATFORM: R0/0: /usr/sbin/pkg_to_tree: Failed to parse the key record 0. (28)
CSCwh42119	Ucode crash when ZBFW is configured on inside interfaces
CSCwf95535	Intf/System xml files are not generated on cEdge
CSCwf99947	Crash when modifying tunnel after running "show crypto" commands
CSCwd16419	C9800-CL-K9 unexpected reload generates pubd core
CSCwd97077	ISR leaking memory in MallocLite because of telemetry subscription to collect FNF cache
CSCwf78735	C8200 uses the NIM-1T/4T card for interconnection, and NAT+ GRE over ipsec cannot be applied
CSCvy94747	GRACEFUL-RELOAD: Wrong state: 1 to recieve chasfs event:
CSCwe37123	8500 Uses Excessive Memory When Configuring ACLs with Large Object Groups
CSCwh30377	ASR1K data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length
CSCwd90056	C8500-12X4QC P2MP WAN MACSEC does not allow traffic to pass on the link
CSCwh45579	Unexpected reload on ASR1k 17.3.5 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 ASR1k won't revoke
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on C1117-4PLTEEA
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 ASR1k to crash

Identifier	Headline
CSCwd05362	Performance issue on ASR900 platform
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted
CSCwe24491	ISR4k : Static NAT with HSRP stops working after removing / adding standby
CSCwf62757	C8500L Interface data report interval issue for physical interface
CSCwf71557	IPv4 connectivity over PPP not restored after reload
CSCwh01738	Unexpected reload when using rsh/rcmd on 17.6
CSCwf59929	CTS CORE process crash after configuring role based ACL
CSCwh35397	Intermittent one way audio on RTP to SRTP calls with SSRC and seq num changes
CSCwh20577	Crashed by TRACK Client thread at access invalid memory location
CSCwe21703	DMI for RESTCONF/NETCONF Enters Degraded State due to Discriminator Configured
CSCvz20285	SDWAN image info not updated in packages.conf when upgrading in autonomous mode
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config
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

Open and Resolved Bugs for Cisco IOS XE Bengaluru 17.6.5a

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool , each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Resolved Bugs for Cisco IOS XE Bengaluru 17.6.5a

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 Bugs for Cisco IOS XE Bengaluru 17.6.5a

Bug ID	Headline
CSCwd79089	Device 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 not sending properly NBAR application information.
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client
CSCwd71458	Outgoing number of bytes decrease in device interface
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

Open and Resolved Bugs for Cisco IOS XE Bengaluru 17.6.5

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool , each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Resolved Bugs for Cisco IOS XE Bengaluru 17.6.5

Bug ID	Headline
CSCvz93612	%HW_FLOWDB-3-HW_FLOWDB_DBLDEL_FEATOBJ: FlowDB featobj cannot be deleted twice
CSCvy60839	CSDL Compliance: Add CLI to disable CSDL compliance
CSCwc82140	QFP Crash When ZBFW Configuration Features log dropped-packets configuration
CSCwc99823	Fman crash seen in SGACL@ fman_sgacl_calloc
CSCwc78021	Standby WLC crash @ fman_acl_remove_default_ace
CSCvz92994	Lack of MAC address in Inform Event message.
CSCwc89328	Device might Reboot when supporting explicit IV joins network
CSCwb52324	Device unexpected reload due to QFP ucode crash
CSCwd05356	Device observing Error %HW_FLOWDB-3-HW_FLOWDB_DBLINSTALL_FEATOBJ
CSCwd61255	Data Plane Crash on device when Making QOS Configuration Changes
CSCwb04815	NHRP process taking more CPU because of FlexVPN event trace
CSCwc22314	Traffic not being rewritten by NAT
CSCwd01326	Device crashes with SIGABRT within cio infra under heavy load
CSCwd30578	Wired guest client stuck at IP_LEARN with dhcp packets not forwarded out of the foreign to anchor
CSCwd71584	DSPware 58.5.2 release

Bug ID	Headline
CSCwb73395	Need CLI option to disable ALG
CSCwd27876	Reload occurring on a device acting as hub FlexVPN when establishing IPSEC tunnels
CSCwc54463	Device is down when high CPU noticed
CSCwc72923	ERROR info: Device 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	Number of lite sessions conversion in progress counter not decrementing on failed account-logon
CSCwd47123	Device uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply
CSCwb32635	Device file is incomplete when running admin-tech
CSCwd72312	GETVPN : Traffic drops seen on GM after rekey installing policies on latest image
CSCwa13926	IOSXE_SPA-3-UNSUPPORTED_DATA: Data conversion error (media type, 0x172)

Open Bugs for Cisco IOS XE Bengaluru 17.6.5

Bug ID	Headline
CSCwd79089	Device 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 not sending properly NBAR application information.
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client
CSCwd71458	Outgoing number of bytes decrease in device interface
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

Open and Resolved Bugs for Cisco IOS XE Bengaluru 17.6.4

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool , each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date

- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Resolved Bugs for Cisco IOS XE Bengaluru 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
CSCwb25137	[XE NAT] Source address translation for multicast traffic fails with route-map
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions
CSCwb32059	Cellular interface tracker down but NAT route persists in the Service VPN Routing Table
CSCvz98547	Device should not show warning message during reload
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 not showing correct values post upgrade
CSCwb43605	Device 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
CSCwa97951	Basic feature template fails on device with TenGig interface due to negotiation auto
CSCwa67886	UDP based DNS resolution doesn't work with IS-IS EMCP on IOS-XE
CSCwb85046	Device reloads when group-range is configured under an interface Group-Async
CSCwc39881	Certificate signing request generated from device contains "/" in common name

Bug ID	Headline
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	Speed test to internet failing on devices
CSCvz99832	Device per class BFD - echo response pkts
CSCwb08636	IPSEC-3-HMAC_ERROR: IPSec SA receives HMAC error seen for TLOCExt setup after upgrade
CSCvx74917	DNS Packets are not redirected to configured custom DNS after Umbrella template edit
CSCwa72273	ZBFW dropping return packets from device post upgrade.
CSCwa98144	No negotiation auto command changing to negotiation auto after reload
CSCwa64955	Device loses control connections after installing new enterprise hardware cert
CSCwa92137	Device is changing ICMP ID in ICMP echo replies intermittently
CSCwa49721	Device 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 device with NAT
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored
CSCwa80826	Device running crypto ipsec policy installation fails
CSCwb83376	Device endpoint-tracker cannot be configured on a 100G interface
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
CSCwb78173	CSDL failure: IPSec QM Use of DES by encrypt proc is denied
CSCwb71658	Traceback seen on devices after enabling ipsec_pwk and reboot
CSCwb76170	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
CSCwb91729	Fix mishandling of policy sequence programming failures and notify with syslog/notification
CSCwc25854	Device ucode crash due to SIGABRT from bnxt_start_xmit
CSCvy54048	CPP unexpected reboot While Freeing CVLA Chunk
CSCwa30857	Internet speed test 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

Bug ID	Headline
CSCwa98545	Checks of route leaks creates memory corruption.
CSCwb46649	NAT translation dont show (or use) correct timeout value for an established TCP session
CSCwa08847	ZBFW policy stops working after modifying the zone pair
CSCwc33311	Device crash @ imgr_n2_ipsec_sa_ctx_register
CSCwb12647	Device crash for stuck threads in cpp on packet processing
CSCwc04688	Device crash observed after enabling NWPI trace with IPv6 traffic
CSCwb78290	CISCO 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	BFD tunnel are zero with device
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 cert does not remove old cert causing device to use old cert
CSCwb51595	Missing IOS config (voice translation rule) on upgrade
CSCwb40575	After upgrade, umbrella DNS config set to NONE in show umbrella config
CSCwb18315	Umbrella DNS security policy doesn't work device with SIG tunnels
CSCwb58468	Sig Autotunnels:tunnel 409 response received
CSCwc04289	Inconsistency between Path MTU Discovery result and Tunnel MTU

Open Bugs for Cisco IOS XE Bengaluru 17.6.4

Bug ID	Headline
CSCwc62269	process may fail to start, control connection may fail as DCONFAIL
CSCwb62474	Device may crash when doing speedtest with WAN flapping
CSCwc27208	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES
CSCwb74821	yang-management process confd is not running
CSCvz92994	Lack of MAC address in Inform Event message.
CSCwc55260	Memory leak due to FTMd process
CSCwc20170	Device reloads unexpectedly due to Critical FTMd Fault when VRF Configuration is Pushed
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCwc59598	Sstatistics collection causing service-side BFD to flap on every collection interval

Bug ID	Headline
CSCwc52538	Device flows are not distributed and load-balanced evenly and consistently
CSCwc22314	Traffic not being rewritten by NAT
CSCwb83236	Traceback: QFP core after pushing data policy with IPv6 interface
CSCwc67465	Device can not be upgraded
CSCwc26669	TLB miss for lock address during FNF cache lookup
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
CSCwc30050	UTD: Exception in utd_logger.py due to missing extra-data in AMP alert
CSCwc23077	Firewall drop seen stating FirewallL4 seen on device
CSCwd36511	Ping fails to VRRP virtual IP address.

Open and Resolved Bugs for Cisco IOS XE Bengaluru 17.6.3a

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool , each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Resolved Bugs for Cisco IOS XE Bengaluru 17.6.3a

Caveat ID Number	Description
CSCvy63924	Telemetry: IOS-XE Controller crashes after using 'show telemetry ietf subscription all' command.
CSCvx40516	ZBFW + NAT: Traffic flow In2Out scenario failed
CSCvy73165	10G interfaces supports multirate:Mismatch in autoneg/speed in sh run and sh sdwan run
CSCwa26509	Shut/no shut of endpoint-tracker attached tunnel, doesn't create probe again on 17.6.2
CSCvz98373	ZBFW : FirewallPolicy drops seen with RTSP traffic in steady state
CSCvz99404	AclDrop seen on non-SDWAN interface after upgrade to 17.6.1
CSCvw67366	Punt keepalive crashed due to bqs related interrupt
CSCvz73202	C8500-12X TCAM parity error - SDRA : CPP crash on scaling to 5K RA sessions
CSCvz71436	Call Placing issue from SCCP phones
CSCvy69846	Guestshell:.py files stored under /home/guestshell are lost after reboot on 1ng device
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
CSCwa10915	Elephant flow will trigger performance monitor exporting more than 50% byte loss
CSCwa36699	Prefetch CRL Download Fails
CSCvz67279	SELINUX-5-Mismatch Log
CSCvz62032	Attach gateways failed in cloud express
CSCvz59621	MKA Session not coming up on EVC
CSCvz87460	MD5 signature does not match failure while upgrading to 17.3(1r) rommon
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.
CSCwa30988	CoS preservation not working for the services EVPL and EPL tunnel
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

Caveat ID Number	Description
CSCvz34668	Static mapping for the hub lost on one of the spokes
CSCvz84437	Unexpected reload due IPV6 UDP fragment header in VxLAN
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 Bugs for Cisco IOS XE Bengaluru 17.6.3a

Caveat ID Number	Description
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	Cannot transfer files
CSCvz98547	Platforms should not show warning message during reload
CSCwb20089	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
CSCwb00533	Traffic is getting dropped/blackholed due to OCE_ADJ_DROP reason.
CSCwa98144	C8500L-8S4X - No negotiation auto command changing to negotiation auto after reload
CSCwb25913	After configuring match input-interface on class-map, router goes into a reboot loop
CSCvz94966	Throughput drop of 10% from 17.3 to 17.6 Release
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.
CSCvz91913	C8500-12X4QC: Bay 2 startup config of 40Gbps not applied on reload
CSCwa68471	Traceback: CPP ucode core generated after HSRP priority change
CSCvz31901	Cisco makefile changes to build the PHY API SW 4.67.05
CSCwa49721	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
CSCvz62601	High CPU on LC process mcpcc-lc-ms and link flaps

Caveat ID Number	Description
CSCwa98545	Checks of route leaks creates memory corruption.
CSCwa94158	C8500 media type is not correct after removing an SFP
CSCvz08674	Device 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	FN980 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
CSCwb32635	File is incomplete when running admin-tech
CSCvz55275	Show DMVPN command displays incorrect state
CSCwa74499	ZBFW seeing the SIP ALG incorrectly dropping traffic and resetting connection
CSCvz95158	IPSec Led doesn't lit even though module is correctly installed
CSCvz74322	"Shutdown" command visible in running config after reload
CSCwb18315	Umbrella DNS security policy doesn't work

Open and Resolved Bugs for Cisco IOS XE Bengaluru 17.6.2

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool , each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Resolved Bugs for Cisco IOS XE Bengaluru 17.6.2

Caveat ID Number	Description
CSCvx08118	ASR1001-X: Bug to further address CSCvt08179 : QFP crash due to hardware interrupt
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
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 won't come up after "ospfv3 authentication ipsec" is applied on Tunnel interface
CSCvy92960	C8500 QFP FirewallNonsession drops when starting 80K flows
CSCvy94954	LA LED turns green when just inserted SFP-10G-LR on ISR4k 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
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.

Caveat ID Number	Description
CSCvz09078	FireWall Policy Drops are seen when the OG/ACE's are reconfigured multiple times
CSCvz09330	Bootstrap aaa config issues due to default aaa config
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
CSCvz25619	FNF: Reload due to a memory allocation failure in cEdge
CSCvz26211	flow monitor statistics missing when reloading with configuration
CSCvz34290	no ip nbar resources flow max-session does not restore default platform session limits
CSCvz45159	Data plane crash seen on C8200-UCPE-1N8 with upgrade of c8kv from 17.5.1 to 17.6.1 build
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.
CSCvz73780	memory leak with fman_cc process when SM-X-G4M2X module installed
CSCvx08118	ASR1001-X: Bug to further address CSCvt08179 : QFP crash due to hardware interrupt
CSCvy24936	vBond connections continuously flapping on edge devices.
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

Caveat ID Number	Description
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 won't come up after "ospfv3 authentication ipsec" is applied on Tunnel interface
CSCvy91411	SD-WAN policy is not correctly programmed in cEdge
CSCvy92960	C8500 QFP FirewallNonsession drops when starting 80K flows
CSCvy94954	LA LED turns green when just inserted SFP-10G-LR on ISR4k 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
CSCvy99344	cEdge: Multicast UnconfiguredIpv4Fia drop when multicast interworks with service chain/NAT DIA
CSCvz00054	CAT8300 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
CSCvz04121	"show sdwan tunnel statistics bfd" and "clear sdwan tunnel statistics" issues
CSCvz06952	vSmart crash on ompd process
CSCvz07134	Router does not boot on recent 16.X releases with large service policy applied on the interface.
CSCvz07542	ISR4K with NIM-ES2 "no igmp snooping vlan x" is not preserved after reload.
CSCvz08449	Cat8kv - 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 config
CSCvz18867	IP NAT source static does not work for TCP traffic from OUT to IN
CSCvz20181	C8500L: Overruns happening when flow-control enabled

Caveat ID Number	Description
CSCvz23024	17.6.1_auto:SNMP failure on bfdSessionsListSystemIp
CSCvz24267	Static NAT entry is injecting a route to Null0
CSCvz25619	FNF: Reload due to a memory allocation failure in cEdge
CSCvz26211	flow monitor statistics missing when reloading with configuration
CSCvz30465	MT: Template push with ThousandEyes feature failed for ISR4461 after PnP workflow
CSCvz34290	no ip nbar resources flow max-session does not restore default platform session limits
CSCvz35812	cedge ISR4221 cpp_cp_svr crash in ZBF component
CSCvz38312	ISR1100 - cedge: Tx queue hang issue on RJ45 ports
CSCvz40788	SDWAN tunnels are not coming up in Multilink Frame relay sub-interface
CSCvz41766	VG450 Crashes Repeatedly in IOSd due to HTSP
CSCvz45159	Data plane crash seen on C8200-UCPE-1N8 with upgrade of c8kv from 17.5.1 to 17.6.1 build
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	ISR4k:BFD scaling: Not able to scale more that 2048 BFD sessions
CSCvz70734	cEdge crash with sdwan overlay multicast: "CPU Usage due to Memory Pressure exceeds threshold"
CSCvz73780	memory leak with fman_cc process when SM-X-G4M2X module installed

Open Bugs for Cisco IOS XE Bengaluru 17.6.2

Caveat ID Number	Description
CSCvv82985	dhcpv6_relay:dhcp-client on branch not receive ipv6 address

Caveat ID Number	Description
CSCvw67366	ASR1002-X: 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
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	ASR 1000 fails to install rekey causing traffic drop
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes
CSCvz31901	ASR 1000: 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	ASR 1001X crash 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
CSCvz62601	ASR1000-MIP100 / IOS XE 17.3.2 / high CPU on LC process mcpcc-lc-ms and link flaps
CSCvz65545	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535
CSCvz67279	SELINUX-5-Mismatch Log on ASR1002HX and 8500 Platforms
CSCvz74322	"Shutdown" command visible in running config after reload of ASR 1002-HX
CSCvz76277	Hostname not allowed beginning with numbers
CSCvz80197	FTMD message error
CSCvz84437	8500L // 17.6.1a// Unexpected reload due IPV6 UDP fragment header in VxLAN
CSCvz87460	ASR 1000-RP2|VID>V07|16.9.7 MD5 signature does not match failure while upgrading to 17.3(1r) rommon
CSCvv82985	dhcpv6_relay:dhcp-client on branch not receive ipv6 address

Caveat ID Number	Description
CSCvw67366	ASR1002-X: 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
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	ASR 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
CSCvz54262	ASR1001X crash 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
CSCvz62601	ASR1000-MIP100 / IOS XE 17.3.2 / high CPU on LC process mcpcc-lc-ms and link flaps
CSCvz65545	ISIS reports encode error when NSF cisco if configured for GRE tunnel number greater than 65535
CSCvz67279	SELINUX-5-Mismatch Log on ASR1002HX and 8500 Platforms
CSCvz74322	"Shutdown" command visible in running config after reload of ASR 1002-HX
CSCvz76277	Hostname not allowed beginning with numbers
CSCvz77008	SDWAN Router Crashed "Critical process qfp_ucode_csx fault on fp_0_0 (rc=139)"
CSCvz80197	FTMD message error
CSCvz84437	8500L // 17.6.1a// Unexpected reload due IPV6 UDP fragment header in VxLAN
CSCvz87460	ASR 1000-RP2|VID>V07|16.9.7 MD5 signature does not match failure while upgrading to 17.3(1r) rommon

Open and Resolved Bugs for Cisco IOS XE Bengaluru 17.6.1a

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool , each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results.

Note If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.

We recommend that you view the field notices for the current release to determine whether your software or hardware platforms are affected. You can access the field notices from the following location:

Product Field Notice Summary

Resolved Bugs for Cisco IOS XE Bengaluru 17.6.1a

Caveat ID Number	Description
CSCvo41609	GETVPN: Clearing members on Key Server causing rekey processing failure on GMs
CSCvw91361	Crash when issuing "show crypto isakmp peers config"
CSCvx11702	C8500-12X4QC: Traffic drops on 10G interface with large packet size 9000bytes with High priority.
CSCvx25217	cannot remove NAT configuration from the template in a single operation if NAT translation is active
CSCvx32670	Wrong reload reason reflected after a power outage.
CSCvx45788	cannot apply ciscosdwan.cfg due to vpg-log-server-acl ACL on VirtualPortGroup0 for logging
CSCvx53399	fman_fp_image crashed with ZBFW config change

Caveat ID Number	Description
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	[17.5] 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
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
CSCvx96496	c8500L platform: USB Drive not getting detected
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
CSCvy32673	C8500-12X4QC /1hx-Interface doesn't come up when reboot/upgrade device with autoneg enabled on 10G SFP+ Port
CSCvy33007	"Best of Worst" Fallback mode causes reachability issue when routes flap
CSCvy33818	On MTT vManage system IP persists after invalidating and deleting the edge devices.

Caveat ID Number	Description
CSCvy34102	CPP ucode crash with route-map and overload at ipv4_nat_rmap_walk_find.
CSCvy37216	vManage fails to push template - interface config stuck
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
CSCvy67720	[FNF] Need to force DTL read after PLU lookup in fnf_build_do_ipv4_fast
CSCvy93830	BFD tunnel uptime not showing correct values post upgrade to 17.6.01

Open Bugs for Cisco IOS XE Bengaluru 17.6.1a

Caveat ID Number	Description
CSCvx95405	Cellular interface lte Network Selection Mode switches to auto following a reload
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
CSCvz06095	ReassTimeout drops with NAT in Port-Channel.
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
CSCvz35967	cEdge reboot due to "Critical process fman_fp_image fault on fp_0_0 (rc=134)"
CSCvz35990	OSPFv3 IPSec encryption failure when IPv4 address-family not configured in VRF

ROMmon Release Requirements

Use the following tables to determine the ROMmon version required for your Catalyst 8500 model:

Table 2: Minimum and Recommended ROMmon Releases

	DRAM	Minimum Rommon	Recommended Rommon
C8500-12X4QC & C8500-12X	16GB(default)	17.2(1r)	17.11(1r)
	32GB	17.2(1r)	17.11(1r)
	64GB	17.3(2r)	17.11(1r)
C8500-20X6C	All variants	17.10(1r)	17.10(1r)
C8500L-8S4X	-	17.8(2r) - available from Cisco IOS XE 17.9.1a release	-
	-	17.10(1r)- available from Cisco IOS XE 17.10.1a release	-

Note In case of C8500L-8S4X platform, the ROMmon image is bundled with the Cisco IOS XE software image which ensures that when the device is booted up, the ROMmon image is also automatically upgraded to the recommended version.

Table 3: ROMmon Release per Platform

C8500-12X4QC & C8500-12X	17.2(1r)
	17.3(1r)
	17.11(1r)
C8500-20X6C	17.10(1r)
C8500L-8S4X	17.8(2r)
	17.10(1r)

Table 4: What's New in the ROMMon Release

ROMmon Release for C8500-12X4QC, C8500-12X	Fixes
17.3(1r)	Supports 64GB DRAM for C8500-12X4QC & C8500-12X
17.10 (1r)	Added support for new platform C8500-20X6C
17.11(1r)	Fixed a issue in data wipe feature

ROMmon Release for C8500L-8S4X	Fixes
17.10(1r)	CSCwa41877 - Fixes for Intel 2021.2 IPU CSCwb67177 - Fixes for Intel 2022.1 IPU CSCwb60723 - Fixes for CPU temperature CSCwb60863- Fixes for TAM_LIB_ERR_WRITE_FAILURE error

Related Documentation

- Hardware Installation Guide for Catalyst 8500 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8500L Series Edge Platforms
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Software Configuration Guide for Catalyst 8500 Series Edge 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 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.