Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Bengaluru 17.6.x

First Published: 2021-08-24

Last Modified: 2024-04-04

Full Cisco Trademarks with Software License

Cisco 4000 Series Integrated Services Routers Overview

Note Cisco IOS XE Bengaluru 17.6.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE Bengaluru 17.6.x release series.

The Cisco 4000 Series ISRs are modular routers with LAN and WAN connections that can be configured by means of interface modules, including Cisco Enhanced Service Modules (SM-Xs), and Network Interface Modules (NIMs).

The following table lists the router models that belong to the Cisco 4000 Series ISRs.

Cisco 4400 Series ISR	Cisco 4300 Series ISR	Cisco 4200 Series ISR
Cisco 4431 ISR	Cisco 4321 ISR	Cisco 4221 ISR
Cisco 4451-X ISR	Cisco 4331 ISR	
Cisco 4461 ISR	Cisco 4351 ISR	

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.

System Requirements

The following are the minimum system requirements:

Note There is no change in the system requirements from the earlier releases.

- Memory: 4 GB DDR3 up to 32 GB
- Hard Drive: 200 GB or higher (Optional). The hard drive is only required for running services such as Cisco ISR-WAAS.
- Flash Storage: 4 GB to 32 GB
- NIMs and SM-Xs: Modules (Optional)
- NIM SSD (Optional)

For more information, see the Cisco 4000 Series ISRs Data Sheet.

Note For more information on the Cisco WAAS IOS-XE interoperability, see the WAAS Release Notes: https://www.cisco.com/c/en/us/support/routers/wide-area-application-services-waas-software/products-release-notes-list.html.

Determining the Software Version

You can use the following commands to verify your software version:

- For a consolidated package, use the **show version** command
- For individual sub-packages, use the **show version installed** command

Upgrading to a New Software Release

To install or upgrade, obtain a Cisco IOS XE Begaluru 17.6.x consolidated package (image) from Cisco.com. You can find software images at http://software.cisco.com/download/navigator.html. To run the router using individual sub-packages, you also must first download the consolidated package and extract the individual sub-packages from a consolidated package.

Note When you upgrade from one Cisco IOS XE release to another, you may see *%Invalid IPV6 address* error in the console log file. To rectify this error, enter global configuration mode, and re-enter the missing IPv6 alias commands and save the configuration. The commands will be persistent on subsequent reloads.

For more information on upgrading the software, see the How to Install and Upgrade the Software section of the Software Configuration Guide for the Cisco 4000 Series ISRs.

Recommended Firmware Versions

The following table lists the recommended ROMMON and CPLD versions for Cisco IOS XE 17.2.x onwards releases.

Table 1: Recommended Firmware Versions

Cisco 4000 Series ISRs	Existing ROMMON	Cisco Field-Programmable Devices	CCO URL for the CPLD Image
Cisco 4461 ISR	16.12(2r)	21102941	isr_4400v2_cpld_update_v20.SPA.bin isr4400v2hwprogrammdbl040100SPA.pkg
Cisco 4451-X ISR	16.12(2r)	19042950	isr4400_cpld_update_v20.SPA.bin
Cisco 4431 ISR	16.12(2r)	19042950	isr4400_cpld_update_v20.SPA.bin
Cisco 4351 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4331 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4321 ISR	16.12(2r)	19040541	isr4300_cpld_update_v20.SPA.bin
Cisco 4221 ISR	16.12(2r)	19042420	isr4200_cpld_update_v20.SPA.bin

Note Cisco 4461 ISR may require two upgrade packages to upgrade to 21102941. See CPLD-4-1 Release Notes.

Upgrading Field-Programmable Hardware Devices

The hardware-programmable firmware is upgraded when Cisco 4000 Series ISR contains an incompatible version of the hardware-programmable firmware. To do this upgrade, a hardware-programmable firmware package is released to customers.

Generally, an upgrade is necessary only when a system message indicates one of the field-programmable devices on the Cisco 4000 Series ISR needs an upgrade, or a Cisco technical support representative suggests an upgrade.

From Cisco IOS XE Release 3.10S onwards, you must upgrade the CPLD firmware to support the incompatible versions of the firmware on the Cisco 4000 Series ISR. For upgrade procedures, see the Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs.

Feature Navigator

You can use Cisco Feature Navigator to find information about feature, platform, and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on cisco.com is not required.

New and Changed Information

New Hardware Features in Cisco IOS XE 17.6.x

There are no new hardware features for 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 2: Software Features in Cisco 4000 Series ISRs Release Cisco IOS XE 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.

Feature	Description
CFM Operation and Action Command Support	This feature introduces a NETCONF/YANG model to perform the following functions: • Display Ethernet CFM maintenance-points data for local MEP, local MIP, remote MEP, or database. • Activate or deactivate CFM latching loopback and start or stop OAM remote loopback. This model helps you to gain more visibility into the timing of the services operations and manage network devices from a centralised orchestration application such as Cisco DNAC. For more information, see the Programmability Configuration Guide.
Cisco ThousandEyes Application	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.
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.
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 Virtual Private Wire Service (VPWS) or Virtual Private LAN Service (VPLS) pseudowire. VPWS or VPLS pseudowires between same PEs can be routed over different SR policies based on the requirements.

Feature	Description

Phasing Out of Device-Specific HSECK9 Licenses	With the introduction of Cisco Digital Network Architecture (Cisco DNA), there is a change in the entitlement tags for HSECK9 licenses supported on Cisco 4000 Series Integrated Services Routers. Instead of tagging licenses according to a router model (for example, ISR_4331_Hsec), HSECK9 licenses are tagged as *Router US Export Lic for DNA (DNA_HSEC)*. Starting with this release, if you want to purchase new HSECK9 licenses for these products, we recommend that you buy only DNA_HSEC.
	
	If the software version running on the product instance is Cisco IOS XE Bengaluru 17.6.1a or later, it has the following implications:
	• A device-specific HSECK9 license that is already IN-USE, continues to be supported and no further action is required.
	• For an *unused* device-specific HSECK9 license in the Smart Account and Virtual Account in CSSM, you can do one of the following to use it on a product instance:
	  • Install SLAC in the offline mode. (Generating and Downloading SLAC from CSSM to a File and Installing a File on the Product Instance)
	  • Convert the device-specific HSECK9 license to DNA_HSEC and then install SLAC according to your topology. The product instance can be connected to CSLU or SSM On-Prem or Cisco VManage or Cisco DNA Center or CSSM. (Converting a Device-Specific HSECK9 License)
	  • Downgrade to a software version where you can install a device-specific HSECK9 license (for example, Cisco IOS XE Amsterdam 17.3.6) and then revert to Cisco IOS XE Bengaluru 17.6.1a or later.
	
	For more information, see Phasing Out of Device-Specific HSECK9 Licenses.

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.
Pyang version 2.x	The updated pyang plugin version 2.x fixes existing issues such as XPATH validation and upstream pyang issues. Additionally, this version reports all errors in the YANG models to the users and enforces a strict model validation.
Redistribution of leaked routes into BGP	This feature allows you to leak (or replicate) routes between the global VRF and service VPNs, and redistribute the leaked routes into the destination protocol BGP. The redistribution of the leaked routes occurs after replicating the routes into the corresponding VRF. Route leaking allows you to share common services that multiple VPNs need to access. The source protocols that support route leaking and redistribution of routes into the destination protocol BGP are as follows: • Connected • Static • BGP • OSPF • EIGRP

Feature	Description
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.

Table 3: Software Features in Cisco 4000 Series ISRs Release Cisco IOS XE 17.6.2

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

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.

Configure the Router for Web User Interface

This section explains how to configure the router to access Web User Interface. Web User Interface requires the following basic configuration to connect to the router and manage it.

- An HTTP or HTTPs server must be enabled with local authentication.
- A local user account with privilege level 15 and accompanying password must be configured.
- Vty line with protocol SSH/Telnet must be enabled with local authentication. This is needed for interactive commands.

- For more information on how to configure the router for Web User Interface, see Cisco 4000 Series ISRs Software Configuration Guide, Cisco IOS XE 17.

Resolved and Open Bugs

This section provides information about the bugs in Cisco 4000 Series Integrated Services Routers and describe unexpected behavior. Severity 1 bugs are the most serious bugs. Severity 2 bugs are less serious. Severity 3 bugs are moderate bugs. This section includes severity 1, severity 2, and selected severity 3 bugs.

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

Resolved and Open Bugs in Cisco 4000 Series Integrated Services Routers

Resolved Bugs - Cisco IOS XE 17.6.7

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Description
CSCwh73350	Router keeps crashing when processing a firewall feature.
CSCwh99399	FTMD crash observed in 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.
CSCwh40504	SM-X interface stops passing traffic.

Bug ID	Description
CSCwi01046	PoE module is not providing enough power to bring the ports after an unexpected reload.
CSCwh20577	Crashed by TRACK client thread at access invalid memory location.
CSCwh70449	PMTUD incorrectly converging without attempting to learn a higher MTU.
CSCwf34171	**configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwh36801	Crash in IP input process during tunnel encapsulation.

Open Bugs - Cisco IOS XE 17.6.7

All open bugs for this release are available in the Cisco Bug Search Tool.

There are no open bugs in this release.

Resolved Bugs in Cisco IOS XE 17.6.6a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z

Open Bugs - Cisco IOS XE 17.6.6a

All open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
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.
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 router may experience unexpected reset while executing **show utd engine standard statistics**.

Bug ID Number	Description
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	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	%IOSXE-3-PLATFORM: R0/0: /usr/sbin/pkg_to_tree: Failed to parse the key record 0. (28).
CSCwa92813	Unexpected reload with segmentation fault due to Open DNS Dev-Reg process.
CSCwf95535	Intf/System XML files are not generated.
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands.
CSCwd16419	Unexpected reload generates pubd core.

Bug ID Number	Description
CSCwc37603	Slot 0/1 crash after changing switchport with allowed wide range VLANs from trunk to access.
CSCwd97077	Device leaking memory in MallocLite 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 recieve chasfs event.
CSCwh12093	SOS/ROC Feature on NIM.
CSCwh30377	Device data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length.
CSCwh50510	Router crash with segmentation fault(11), Process = NHRP when processing NHRP traffic.
CSCwf34171	**configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwh45579	Unexpected reload on 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 device won't revoke.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.
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 platform.
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.
CSCwh40504	SM-X interface stops passing traffic.
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.

Bug ID Number	Description
CSCwh20577	Crashed by TRACK Client thread at access invalid memory location.
CSCwe21703	DMI for RESTCONF/NETCONF enters degraded state due to discriminator configured.
CSCwh01738	Unexpected reload when using RSH/RCMD.
CSCwe26895	Router has LocalSoftADR crash, writes flat core, and reloads.
CSCvz20285	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.
CSCwe24491	Static NAT with HSRP stops working after removing / adding standby.
CSCwd94495	SSM On-Prem responds with message **completed** to poll_id requests without ACK data.

Resolved Bugs - Cisco IOS XE 17.6.6

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
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.
CSCwh08434	OMP route is being advertised although the route is not available.
CSCwd90168	Unexpected reload after running **show voice dsp** command while an ISDN call disconnects.
CSCwe60059	Crash when using dial-peer groups with STCAPP.
CSCwe24210	SNMP MIB does not show correct firmware version.
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.

Bug ID Number	Description
CSCwe07055	Device frequent reloads.
CSCwd88554	Filesystem leak on standby switch of device SVL setup.
CSCwe20008	SNMP MIB OID changing its last index.
CSCwf00769	L2RIB thread crash after removing EVPN member from bridge domain.
CSCwf39552	Segmentation fault by process mDNS.
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	Router 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.
CSCwe52796	Intermittent one way audio issue after hold and resume. SRTP to RTP.
CSCvz12193	snmpwalk: Authentication failure, with MD5 SNMPv3 user.
CSCwd09685	Memory leak found @nfra/green/cep/src/cep.c.
CSCwe64213	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 RSA keypair.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwe33793	Memory allocation failure with extended antireplay enabled.
CSCwc24044	IOS XE device may experience an unexpected reset with High Volume of Multicast.

Bug ID Number	Description
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.
CSCwe10905	vBond tracker.
CSCwd59423	Unexpected reload on device caused by WNCD process after removing a VLAN from a VLAN-GROUP.
CSCwb47153	Keyman process crash.
CSCwf44649	LISP failed to recreate the more specific away table entries after less specific entries toggled.
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 certian options are enabled in configuration.
CSCwf56463	IOS process crash during VRRP hash table lookup.
CSCwf32156	ATTN-3-SYNC_TIMEOUT after upgrading.
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 device by adding tailf:hidden full 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	Device 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.

Bug ID Number	Description
CSCwe37184	Device seeing out of service when using new DC power supply.
CSCwe41234	Device VMWI race condition causes no ringing for analog phones.
CSCwf55830	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	Device 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	Device memory leak in pubd causes reload.
CSCwf27815	DSP resource can not be release after end the call.
CSCuq20562	ISDN memory leak when PRI link flaps, crashes router.
CSCvz55275	**show DMVPN** command displays incorrect state.
CSCwf03292	I/O middle pool leaking when VOIP trace is enabled.
CSCwe66318	NAT entries expire on standby router.
CSCwf01986	Radius attribute 31 not being sent on device for CTS Pac provisioning.
CSCwe39011	GARP on port up/up status from router is not received by remote peer. device.
CSCwf14589	IOS-XE device 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.
CSCwh04884	VC down due to control-word negotiation.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit.
CSCwd49177	ISG: L2-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 Bugs - Cisco IOS XE 17.6.6

All open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
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.
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 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	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.

Bug ID Number	Description
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	%IOSXE-3-PLATFORM: R0/0: /usr/sbin/pkg_to_tree: Failed to parse the key record 0. (28).
CSCwa92813	Unexpected reload with segmentation fault due to Open DNS Dev-Reg process.
CSCwf95535	Intf/System XML files are not generated.
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands.
CSCwd16419	Unexpected reload generates pubd core.
CSCwc37603	Slot 0/1 crash after changing switchport with allowed wide range VLANs from trunk to access.
CSCwd97077	Device leaking memory in MallocLite 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 recieve chasfs event.
CSCwh12093	SOS/ROC Feature on NIM.
CSCwh30377	Device data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length.
CSCwh50510	Router crash with segmentation fault(11), Process = NHRP when processing NHRP traffic.
CSCwf34171	**configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwh45579	Unexpected reload on 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 device won't revoke.

Bug ID Number	Description
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.
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 platform.
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.
CSCwh40504	SM-X interface stops passing traffic.
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.
CSCwh01738	Unexpected reload when using RSH/RCMD.
CSCwe26895	Router has LocalSoftADR crash, writes flat core, and reloads.
CSCvz20285	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.
CSCwe24491	Static NAT with HSRP stops working after removing / adding standby.
CSCwd94495	SSM On-Prem responds with message **completed** to poll_id requests without ACK data.

Resolved Bugs in Cisco IOS XE 17.6.5a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z

Open Bugs - Cisco IOS XE 17.6.5a

All open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
CSCwd79089	Device controller crash when sending Full line rate of traffic with >5 Intel AX210 stations.
CSCwd90168	Unexpected reload after running **show voice dsp** command while an ISDN call disconnects.
CSCvq81894	Check nexthop reachability before installing route for a prefix.
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site.
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client.
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCvz55275	**show dmvpn** command displays incorrect state.
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M).
CSCwd71458	Outgoing number of bytes decrease in router interface.
CSCwc56033	Not triggering any alarms when RPM of a fan is 0.
CSCwc37603	Slot 0/1 crash after changing switchport with allowed wide range VLANs from trunk to access.
CSCwd49177	L2-connected subscriber: IPv6 prefix delegation is not reachable when packet are switched.

Resolved Bugs - Cisco IOS XE 17.6.5

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
CSCvz93612	%HW_FLOWDB-3-HW_FLOWDB_DBLDEL_FEATOBJ: FlowDB featobj cannot be deleted twice.
CSCvy60839	CSDL Compliance: Add CLI to disable CSDL compliance.

Bug ID Number	Description
CSCwc82140	QFP crash when ZBFW configuration features log dropped-packets configuration.
CSCwd16664	GetVPN long SA - GM re-registration after encrypting 2^32-1 of packets in one IPSEC SA.
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 the network.
CSCwb52324	Device unexpected reload due to QFP ucode crash.
CSCwd71584	DSPware 58.5.2 release.
CSCwd61255	Data Plane crash on device when making QoS configuration changes.
CSCwb04815	NHRP process taking more CPU because of FlexVPN event trace.
CSCwc22314	RTSP Traffic not being rewritten by NAT.
CSCwd30578	Wired guest client stuck at IP_LEARN with dhcp packets not forwarded out of the foreign to anchor.
CSCwd56131	LTE modem doesn't show GSM bands.
CSCwb73395	Need CLI option to disable ALG.
CSCwc54463	LAN 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	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	File is incomplete when running admin-tech.
CSCwd72312	GETVPN : Traffic drops seen on GM after rekey installing policies.

Open Bugs - Cisco IOS XE 17.6.5

All open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
CSCwd79089	Device controller crash when sending Full line rate of traffic with >5 Intel AX210 stations.
CSCwd90168	Unexpected reload after running **show voice dsp** command while an ISDN call disconnects.
CSCvq81894	Check nexthop reachability before installing route for a prefix.
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site.
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client.
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCvz55275	**show dmvpn** command displays incorrect state.
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M).
CSCwd71458	Outgoing number of bytes decrease in router interface.
CSCwc56033	Not triggering any alarms when RPM of a fan is 0.
CSCwc37603	Slot 0/1 crash after changing switchport with allowed wide range VLANs from trunk to access.
CSCwd49177	L2-connected subscriber: IPv6 prefix delegation is not reachable when packet are switched.

Resolved Bugs - Cisco IOS XE 17.6.4

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
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 crash.
CSCwb25137	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.

Bug ID Number	Description
CSCwa92082	RG B2B(Box to Box), Interchassis HA, STBY is stuck in STANDBY COLD-BULK.
CSCvz98547	Platforms 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	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.
CSCwb03662	CDP/LLDP not working when 10GE interface enabled with MACsec.
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 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	Speed Test to internet failing.
CSCvz99832	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 tunnel post upgrade.
CSCwb55683	Large number of IPSec tunnel flapping occurs when underlay is restored.

Bug ID Number	Description
CSCwa64955	Device loses control connections after installing new enterprise hardware wan edge cert.
CSCwa92137	Device is changing ICMP ID in ICMP echo replies intermittently.
CSCwa49721	HUB with firewall configured incorrectly dropping return packets when routing between VRFs.
CSCwb38501	Support IGMP on voice vlan.
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.
CSCwb23043	MACsec not working on subinterfaces using dot1q >255.
CSCwb16723	Traceroute not working on device with NAT.
CSCwb08186	E1 R2 - dnis-digits cli not working.
CSCwa80826	IOS-XE: Devices running crypto ipsec policy installation fails.
CSCwb83376	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.
CSCwa57462	The router reload unexpectedly due to Cellular CNM process.
CSCwb71658	Traceback after enabling ipsec_pwk and reboot.
CSCwb41907	CPP uCode crash due to ipc congestion from dp to cp.
CSCwb74917	Device incorrectly drops ip fragments due to reassembly timeout.
CSCwc25854	ucode crash due to SIGABRT from bnxt_start_xmit.
CSCwb77202	Interface comes up with only an SFP inserted.
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.

Bug ID Number	Description
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.
CSCwc33311	Device crash @ imgr_n2_ipsec_sa_ctx_register.
CSCwa26599	FN980 new signed Telit modem firmware FN980M_38.02.X92 upgrade failed.
CSCwb12647	Device crash for stuck threads in cpp on packet processing.
CSCwc04688	Device crash observed after enabling NWPI trace with IPv6 traffic.
CSCwb76170	IPsec SIG auto tunnels are not coming up.
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.
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 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 with Cloud onRamp with SIG tunnels.
CSCwb58468	Sig Autotunnels:tunnel 409 response received.
CSCwc04289	Inconsistency between Path MTU Discovery result and Tunnel MTU.
CSCwb78290	CISCO-SDWAN-BFD-MIB request gives results intermittently.
CSCwc88439	Device bootflash breakage unable to format bootflash.
CSCwa51443	Incorrect check of the TCP sequence number causing return ICMP error packets to drop (Thousandeyes).
CSCwa85199	High CPU utilization and memory utilization by Smart Licensing Agent.

Open Bugs - Cisco IOS XE 17.6.4

All open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
CSCwc25291	NIM-LTE-EA No Data - Requires subslot reload to recover.
CSCwc55260	Memory leak due to FTMd process.
CSCwc63563	Unable to set specific speed and duplex values on SFP ports on IOS-XE routing platforms.
CSCwb99084	OMP routes carrying prepended AS_PATH incorrectly imported into BGP at remote site.
CSCwc30050	UTD: Exception in utd_logger.py due to missing extra-data in AMP alert.
CSCwb89958	Unified Policy HSL not sending properly NBAR application information.
CSCwb62474	Device may crash when doing speedtest with WAN flapping.
CSCwc52538	Device flows are not distributed and load-balanced evenly and consistently.
CSCwc23077	Firewall drop seen stating “FirewallL4”.
CSCwc22314	RTSP traffic not being rewritten by NAT.
CSCwb74821	Yang-management process confd is not running in controller mode.
CSCwc67465	Router can not be upgraded.
CSCwb83236	Traceback: QFP core after pushing data policy with IPv6 interface.
CSCwc56033	Not triggering any alarms when RPM of a fan is 0.
CSCwc59598	Statistics collection causing service-side BFD to flap on every collection interval.
CSCvz92994	Lack of MAC address in Inform Event message.
CSCwc19533	CRC errors seen after upgrade.
CSCwc27208	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES.
CSCwc53885	IOS-XE no ip nat config is allowed to be committed and removes nat routes among other nat config.
CSCwd36511	Ping fail to VRRP virtual IP address.

Resolved Bugs - Cisco IOS XE 17.6.3a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
CSCwa82825	4461 Sub-interface may not forward traffic after a reload.

Bug ID Number	Description
CSCvy63924	Telemetry: IOS-XE Controller crashes after using 'show telemetry ietf subscription all' command.
CSCwa13553	QFP core due to NAT scaling issue.
CSCvx40516	17.5 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	SdwanImplicitAclDrop seen on non-SDWAN interface after upgrade to 17.6.1.
CSCvw67366	Punt keepalive crashed due to bqs related interrupt.
CSCvz73202	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.
CSCwa30988	CoS preservation not working for the services EVPL and EPL tunnel.
CSCwa36699	Prefetch CRL download fails.
CSCvz67279	SELINUX-5-Mismatch Log.
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.

Bug ID Number	Description
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.
CSCvz84437	17.6.1a// 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 - Cisco IOS XE 17.6.3a

All open bugs for this release are available in the Cisco Bug Search Tool.

Bug 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	CG522: Cannot transfer files.
CSCwa92082	RG B2B (Box to Box), Interchassis HA, STBY is stuck in STANDBY COLD-BULK on ISR 4461.
CSCvx74917	[17.5 Umbrella] DNS Packets are not redirected to configured Custom DNS after Umbrella Template Edit.
CSCwb03662	ISR4461: CDP/LLDP not working when 10GE interface enabled with MACSEC.
CSCwb00533	cEdge traffic is getting dropped/blackholed due to OCE_ADJ_DROP reason.
CSCwb25913	(Rework): 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	Bay 2 startup config of 40Gbps not applied on reload.

Bug ID Number	Description
CSCwa68471	Traceback: CPP ucode core generated after HSRP priority change.
CSCvz31901	Cisco makefile changes to build the PHY API SW 4.67.05.
CSCwa49721	SDWan 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.
CSCwa57462	The router reload unexpectedly due to Cellular CNM process.
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes.
CSCvy54048	CPP unexpected reboot while freeing CVLA chunk.
CSCvz62601	IOS XE 17.3.2 / high CPU on LC process mcpcc-lc-ms and link flaps.
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	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.
CSCwb32635	17.6.2 IOS XE SD-WAN - vdaemon 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 with Cloud onRamp.

Resolved Bugs - Cisco IOS XE 17.6.2

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
CSCvt35331	Console port goes unresponsive, reboot required to restore it.
CSCvy94954	LA LED turns green when just inserted SFP-10G-LR on ISR4k without cable connecting.
CSCvy96872	IP Phone in Voice vlan can't get IP via DHCP if DHCP snooping enabled.
CSCvz00054	Nested IPSec tunnels encryption does not work as expected.
CSCvz47421	VLAN IP config missing on bootup due to missing startup configs.

Open Bugs - Cisco IOS XE 17.6.2

All open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
CSCvy83674	Promethium: Observing low performance compare to UP performance numbers.
CSCvz21267	ISR 4K running in sdwan controller mode experiencing module reload due to NGIO control packet loss.
CSCvz31260	DP CPU degradation in Collab and Contact center flows on ISR4451 platform on 17.3 throttle.
CSCvz37661	17.6 to 17.7: Continious 4461 Octean crypto crash. does not stay up.
CSCvz69124	ISR4k:BFD scaling: Not able to scale more that 2048 BFD sessions.
CSCvz81428	SIT: vedaemon assert noticed in the ISR 4221 over weekend longevity.
CSCvz88205	Buffer Leak - IPSEC reply msg getting dropped.
CSCvz89354	Router running 17.x.x crashes due to CPUHOG when walking CiscoFlashMIB.
CSCvz92383	IPv6 connectivity issues on the service side.
CSCvz93376	ISR prefixing F's to h323-conf-id field.

Resolved Bugs - Cisco IOS XE 17.6.1a

All resolved bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
CSCvy02029	C8000v new PAYG Azure Cloud deployments do not boot with correct throughput level and tech package.
CSCvx07578	ISR4461: MACsec should secure mode not work with front panel GE.
CSCvx15820	Subslot module C1111-ES-8 going "out of service".
CSCvx53399	fman_fp_image crashed with ZBFW config change.

Bug ID Number	Description
CSCvx57615	ZBFW blocking ACK packets for applications using cloudexpress SaaS set to use a Gateway with synsent.
CSCvx59899	ISR4431/K9 rebooting due to CPP crashing becaue of UTD feature.
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.
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".
CSCvy00963	On vManage 20.4.1, traceroute on cEdge leads to outage at the site.
CSCvy01097	Router may crash under ZBF configuration (cpp_cp_svr).
CSCvy13735	BFD tunnels stuck in down state after port-hop.
CSCvy14126	ISR4331 are crashing frequently 17.4.1b.
CSCvy20588	CSDL failure when it should be allowing RSA keys with 1024 length.
CSCvy30209	IOS-XE cpp ucode crash with fragmented packets.
CSCvy31298	ISR4461 NIM-2GE-CU-SFP - Sub-interfaces not transmitting traffic.
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.
CSCvy54314	Data-policy local-tloc with app-route is dropping packets when SLA is not met.
CSCvy64180	ccedge C1121-4P crahed with Localsoft error.
CSCvy67301	URL Filtering regex pattern match not working on large pattern.

Bug ID Number	Description
CSCvy85141	tdm-group timeslot 31 failed to create/connect.
CSCvy93830	BFD tunnel uptime not showing correct values post upgrade to 17.6.01.
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).
CSCvw42048	c1111 vtcp may cause packet drop for sip packets causing phones to reset.
CSCvw91361	Crash when issuing "show crypto isakmp peers config".
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.
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.
CSCvx79113	SDWAN cedge : traffic simulation tool shows traffic blackhole.
CSCvx94323	NHRP messages tagged with incorrect MPLS labels - unable to establish shortcut.
CSCvx97490	ISR4321 | After enabling "cts manual" the interfaces start flapping.
CSCvx97718	vtcp frees rx buffer when packet with expected next sequence arrives with no payload; phones reset.
CSCvy03584	cEdge fails to capture sdwan-related outputs to admin-tech.
CSCvy09777	cEdge running 17.4.1b crashing with NAT Backtraces everytime we shut no-shut PPPoE.
CSCvy10159	Software MTP should support encrypted TLS connection.
CSCvy32935	UTD: Pickup latest SPPI library with fix for CSCvy00963.
CSCvy33007	"Best of Worst" Fallback mode causes reachability issue when routes flap.
CSCvy37216	vManage fails to push template - interface config stuck.
CSCvy52359	Segmentation fault(11), Process = CTS CORE - crash in ISR 4K.
CSCvy52761	Adding multilink frame relay sub-interface to SDWAN fails; "Aborted: application error".
CSCvy78123	cEdge: High CPU usage due to Multicast and Data Policy configuration.

Bug ID Number	Description
CSCvy87803	ISR1K // ethernet loopback not working.

Open Bugs - Cisco IOS XE 17.6.1a

All open bugs for this release are available in the Cisco Bug Search Tool.

Bug ID Number	Description
CSCvy79833	cEdge: Cellular related AOM pending objects after IOS-XE upgrade.
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.
CSCvz08674	cEdge rebooted 2 time with CPP 0 failure Stuck Thread.
CSCvz09078	FireWall Policy Drops are seen when the OG/ACE's are reconfigured multiple times.
CSCvz11158	Not able to upgrade cEdge from vManage | from 16.12.3 to 17.3.3.
CSCvz13126	Ucode crash with test calls from the SIP trunk to the POTS lines.
CSCvz25403	NetApp: Issues with traffic does not get forwarded via TLOC extended interface.
CSCvz33108	After uploading the serial file list to the vmanage, the edges lost Control Con. and BFD sessions.
CSCvz35812	cEdge ISR4221 cpp_cp_svr crash in ZBF component.
CSCvz37551	Switchport Feature Template is unable to create VLANs- Missing VLANs on VLAN-database.
CSCvz40788	SDWAN tunnels are not coming up in Multilink Frame relay sub-interface.
CSCvz41766	VG450 Crashes Repeatedly in IOSd due to HTSP.
CSCvx17563	ISR4331/K9 running 16.12.04 crashed with Segmentation fault(11), Process = Cellular CNM.
CSCvy80013	ISR4K/NIM-4G-LTE-GA 17.3.2 Cellular interfaces automatically unshut after reboot.
CSCvy80452	Router getting %CELLWAN-2-DYING_GASP_POWER_FAILURE without feature configured.
CSCvy87507	Router unexpectedly routes traffic with broadcast dst MAC.
CSCvz28795	SSL VPN fails to establish if 'match url' is configured under crypto ssl profile.
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes.

Bug ID Number	Description
CSCvz35990	OSPFv3 IPSec encryption failure when IPv4 address-family not configured in VRF.

Related Documentation

- Release Notes for Previous Versions of Cisco 4000 Series ISRs
- Hardware Installation Guide for Cisco 4000 Series Integrated Services Routers
- Configuration Guides for Cisco 4000 Series ISRs
- Command Reference Guides for Cisco 4000 Series ISRs
- Product Landing Page for Cisco 4000 Series ISRs
- Datasheet for Cisco 4000 Series ISRs
- Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs
- Field Notices
- Cisco Bulletins

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.