Release Notes for Cisco 4000 Series ISRs, Cisco IOS XE Dublin 17.12.x

First Published: 2023-08-22

Last Modified: 2024-08-16

Full Cisco Trademarks with Software License

Cisco 4000 Series Integrated Services Routers Overview

Note Cisco IOS XE Dublin 17.12.1a is the first release for Cisco 4000 Series Integrated Services Routers in the Cisco IOS XE 17.12.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).

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 17.12.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 Installing 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 isr4400v2hwprogrammbb040100SPA.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 and Changed Hardware Features

There are no new hardware features for this release.

New and Changed Software Features in Cisco IOS XE 17.12.2

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.

Table 2: New Software Features

Feature	Description
Cisco Managed Cellular Activation (eSIM)	The Managed Cellular Activation solution provides a programmable subscriber identity module (SIM), called an eSIM, a physical SIM card that you can configure with a cellular service plan of your choice. When ordering a pluggable interface module (PIM) to provide cellular connectivity for your router, choose a PIM model with a preinstalled eSIM. The Managed Cellular Activation solution comes with a "bootstrap" cellular plan to provide internet connectivity with a limited amount of data intended only for Day 0 onboarding of the device to your cellular plan. For information about configuring Cisco SD-WAN Manager with the details of your cellular plan in preparation for onboarding the device, see the Cisco Managed Cellular Activation Configuration Guide. Prepare the configuration in Cisco SD-WAN Manager before powering on and onboarding the device, to avoid running out of the limited data in the bootstrap cellular plan. Added Cisco Managed Cellular Activation (eSIM) support for the following Pluggable Interface Module (PIM) model: • 5G Sub-6 GHz PIM, model P-5GS6-R16-GL **Note** In this context, eSIM refers to a removable SIM pre-installed by Cisco. In other contexts, eSIM can refer to a non-removable SIM embedded in a cellular-enabled device.

New and Changed Software Features in Cisco IOS XE 17.12.1a

Table 3: New Software Features in Cisco IOS XE 17.12.1a

Feature	Description
End-of-Sale and End-of-Life Announcement for the Cisco 4000 Series Integrated Service Routers	See the End-of-Sale and End-of-Life Announcement for the Cisco ISR4200, ISR4300 and select ISR4400 Series Platform page for information about the end-of-life milestones for the Cisco 4000 Series Integrated Service Routers.
Managing the SD-Routing Devices Using Cisco SD-WAN Manager	This feature allows you to perform management operations for SD-Routing devices using Cisco Catalyst SD-WAN Manager. You can use a single network manage system (Cisco Catalyst SD-WAN Manager) to monitor all the SD-Routing devices and therefore help in simplifying solution deployments.
Support for Automatic Log Deletion	This feature allows you to delete the entries from the logging buffer. You can configure the local syslog retention period after which the entries are purged from the device automatically. To enable this feature, use the **logging purge-log buffer days** command.

Feature	Description
Support for Secure Factory Reset	This feature introduces the **factory-reset all secure** command for Cisco 4000 Series ISRs. From Cisco IOS XE 17.12.1a, you can use the **factory-reset all secure** command to securely clear all the data in bootflash, hard disk, and ROMMONs.
Cisco Unified Border Element (CUBE) Features	
GCM Ciphers for WebSocket-based Media Forking	From Cisco IOS XE Dublin 17.12.1a onwards, GCM cipher negotiation supports secure connectivity of WebSocket server.
IPv6 Flows in High Availability	From Cisco IOS XE Dublin 17.12.1a onwards, High Availability in CUBE supports IPv6 flows.
Cover Buffer Enhancements for VoIP Trace	From Cisco IOS XE Dublin 17.12.1a onwards, VoIP Trace for SIP messages displays cause code in the cover buffer.

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 17.12.4

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

Bug ID	Description
CSCwj70335	Crypto IKEv2 - Fragmented authentication packets detected as malformed on 3rd-party vendor device.
CSCwj74260	Default setting of Global Punt Policer burst needs to be increased.
CSCwj44868	GETVPN COOP KS | Wrong severity for rekey acknowledgement configuration mismatch log message.
CSCwi16716	Router crashed upon increasing the gatekeeper cache size.
CSCwi88969	FMFP-3-OBJ_DWNLD_TO_DP_FAILED observed when delete and configure zone-pair back.
CSCwj21653	Kernel crash over continuous reloads.
CSCwi68865	Memory leak in crypto IKEv2 due to C_NewObject.
CSCwj09284	Unexpected reboot in WLC due to SSL.
CSCwi40603	Memory leak in the Crypto IKMP process.
CSCwi82405	mGRE tunnels with shared IPsec profile cause ucode crash.
CSCwj34578	NAT46 translations are dropped when NAT64 router is also Carrier Supporting Carrier CE.
CSCwi55183	**crypto pki certificate pool** in running configuration.
CSCwk15127	Failure to communicate a period of time after the STP status changes.
CSCwh37024	PnP gets stuck when Verizon cellular backhaul is used.

Bug ID	Description
CSCwj45130	Segmentation fault - process = IPSec dummy packet process.
CSCwj88872	IPsec tunnel fails to establish due to error IPSec policy invalidated proposal.
CSCwj73113	MGCP GW does not respond with 250 OK for a DLCX leading to DLCX loop from CUCM side.
CSCwi59854	**show sdwan policy service-path** command gives inconsistent results with app name specified.
CSCwj38106	Only one split-exclude subnet is pushed to client PC with IOS-XE headend for a RA VPN connection.
CSCwh73320	NAT Pool does not work under prefix 16. Available address = zero.
CSCwi89822	Unexpected reboot due to CPP ucode.
CSCwi78060	Woodlawn SM-X - Marvell Phy Errata + MAC reset adjustment.
CSCwf87975	Router crashed when port-channel interface flap with scale of per-tunnel QoS policies.
CSCwh86053	ENH: Config parser issue for NAT with extendable and redundancy.
CSCwj42249	Disabling PMTU-Discovery with MTU change and BFD flap breaks packet duplication.
CSCwj36915	C-NIM-2T: MACsec not working under LACP port-channel member port.
CSCwi78365	Trim installed certificate on upgrade.
CSCwj72888	Reload in tcp_sanity due to l4 pointer not set.
CSCwj49297	Device sends out BYE message with high RTT to CUCM (64.2.0/62.3.2/60.1.3).
CSCwi93784	FW upgrade does not work properly on P-LTE-MNA.
CSCwj33292	AnyConnect connection trough IPSec fails when connecting from an RDP user to an IOS/IOS-XE headend.
CSCwj06622	Segmentation fault and core files are seen on IOS-XE due to speedtest.
CSCwi16111	**ipv6 tcp adjust-mss** not working after delete and reconfigure.
CSCwi66850	C-SM-16P4M2X stuck in bootloop when **platform urpf** command issued.
CSCwj29947	AAA authorization failure during IKEv2 phase negotiation caused unexpected reboot.
CSCwj79197	Unexpected reload when using the packet trace feature.

Open Bugs - Cisco IOS XE 17.12.4

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

Bug ID	Description
CSCwk53231	Front Panel (FPGE) Interface stops passing traffic.
CSCwi03502	Create CLI to push at#enadis=0 followed with at#reboot to FN980 required when configuring Multi-PDN.
CSCwk31560	NAT Command not readable after reloaded.
CSCwk03686	Crash due a segmentation fault due a negative value.
CSCwk44078	GETVPN / Migrating to new KEK RSA key does not trigger GM re-registration.
CSCwj06950	DSL module gets stuck in a booting state.
CSCwk18913	IOS-XE crash due to VFR fragment reassembly on ingress.
CSCwk53296	UCSE interface's shutdown setting mismatch.
CSCwj21653	Kernel crash over continuous reloads.
CSCwi31110	Traceback seen @_nhrp_cache_delete due to negative global cache count.
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.
CSCwk58303	Watchdog crash during IPv6 cef adjacency routines.
CSCwk63722	Startup configuration failure post PKI server enablement.
CSCwj77594	WAN IP is allowed to be configured as SYSTEM IP.
CSCwk54544	ZBFW TCAM misprogramming after rules are reordered.
CSCwb47658	Repeated and endless messages "Network change event - activated 4G Carrier Aggregation."
CSCwj90614	High CPU utilisation for confd_cli.
CSCwi53951	Packets with unicast MAC get dropped on a port channel L2 Sub-intf after a router reboot.
CSCwj92560	STCAPP command removed from VG410 after reload.
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwh45389	Key manager crash after hostname change with usage keys.
CSCwk12524	Device reloaded due to ezManage mobile app service.
CSCwk53680	Inbound calls through VG400 results in phantom calls (64.3.0, 60.1.4, 62.3.3).
CSCwk65071	Unexpected reboot due to IOSXE-WATCHDOG DBAL EVENTS after cellular interface flap.

Bug ID	Description
CSCwf91481	Device crashed unexpectedly after a successful WGB/AP config deployment from OD.
CSCwi96187	P-5GS6-GL FN980 modem fW upgrade failing with two modems.
CSCwh91136	IOS XE: Traffic not encrypted and droped over IPSEC SVTI tunnel.
CSCwk52677	DSL router crashing due to %PLATFORM-3-ELEMENT_CRITICAL memory level / iomd process.
CSCwj84949	Unencrypted traffic due to non-functional IPsec tunnel in FLEXVPN hub & spoke setup.
CSCwk30527	IKEv2 session is down after reload if identity local address is assigned to interface.

Resolved Bugs - Cisco IOS XE 17.12.3a

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

Bug ID	Description
CSCwk21189	Template attach fail with unknown element: ssh-version in /ios:native/ios:ip/ios:ssh
CSCwk20843	PPPoE with NAT DIA feature validation failed post upgrade.

Resolved Bugs - Cisco IOS XE 17.12.3

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.
CSCwh18120	IKEv2 - diagnose feature is taking 11% CPU during session bring up.
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCwi28227	NAT HSL logging vrf-filter not working.
CSCwi01046	PoE module is not providing enough power to bring the ports after an unexpected reload.
CSCwh77221	SNMP unable to poll SDWAN Tunnel Data after a minute.
CSCwh96578	SKA_PUBKEY_DB leak in TDL.
CSCwh69765	Security policy w/IPS external syslog config failing generation.
CSCwi06843	Endpoint tracker triggers a CPU hog.
CSCwi33168	DSP reporting out of range utilization values in SNMP.

Bug ID	Description
CSCwh87619	ZBFW is not able to detect packets on TenGig interface.
CSCwh10813	Add verbose log to indicate grant ra-auto un configures grant auto in PKI server.
CSCwi44581	Wireless config not pushing to EWC.
CSCwh40504	SM-X interface stops passing traffic.
CSCwh40073	Interoperability issue between Cisco ISR and Juniper ACX/MX devices with a direct fiber connection.
CSCwh93257	Device creates crooked NAT entry if 2 or more IP phone from NAT outside register to same server.
CSCwi59121	Mobile-app causing excessive authorization attempts with a Null Username.
CSCwi08171	Router may crash due to Crypto IKMP process.
CSCwi49231	VG410 audio loss for 4 seconds.
CSCwi06404	PKI crash after failing a CRL fetch.
CSCwh50510	Router crash with segmentation fault(11), process = NHRP when processing NHRP traffic.
CSCwh75800	CUBE router unexpectedly reloads while fetching certificate Trustpool for SIP TLS.
CSCwi49240	One-Way RTP Issue including DSP Timeout Messages (63.2.0 / 62.3.1).
CSCwi28781	EPBR will generate error when the policy is added and deleted multiple times.
CSCwh73202	IOS-XE unexpected reboot due to critical process qfp_ucode_utah fault on fp_0_0 (rc=139).
CSCwh45169	Unexpected reboot while dispalying information from cleared SSS session.
CSCwh70449	PMTUD incorrectly converging without attempting to learn a higher MTU.
CSCwh96415	Cannot disable DMVPN logging.
CSCwi25737	Router should discard IKE Notification messages with incorrect DOI.
CSCwh50628	Race condition crash on IOS-XE device.
CSCwf86207	Frame relay DTE router crashes due to EXMEM exhaustion.
CSCwh72869	cpp_mcplo_ucode crash with port-channel and NAT.
CSCwh99399	FTMD crash observed in ENCS platform while running PWK suite.
CSCwi79584	Fail to upgrade device due to error: System config has been modified.

Bug ID	Description
CSCwi76087	ATO: Session fails to come up with tunnel its shut no shut in loop(cable unplug-plug in customer) .
CSCwi55379	IPsec traffic is being dropped when PPK is implemented.
CSCwi63042	Packet drops observe between LISP EID over GRE tunnel.
CSCwi18456	No voice in 3-way conference.
CSCwi30529	AAA: Template push fail when aaa authorization is set to local.

Open Bugs - Cisco IOS XE 17.12.3

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

Bug ID	Description
CSCwi03502	Create CLI to push at#enadis=0 followed with at#reboot required when configuring Multi-PDN.
CSCwj08744	Unexpected reload when using **show running-config full | format**.
CSCwi16111	**ipv6 tcp adjust-mss** not working after delete and reconfigure.
CSCwi46997	NAT command not readable after reloaded.
CSCwi67621	Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69).

Resolved Bugs - Cisco IOS XE 17.12.2

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

Bug ID	Description
CSCwf82676	CPU usage mismatch in **show sdwan system status** vs **show proc cpu platform**.
CSCwf55830	No dial tone on analog phones due to DSP going into Power Denial state.
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwf84960	LED L remains green after port shutdown.
CSCwf26875	Ten0/0/2 from port-channel going to suspended status applying **platform qos port-channel-aggregate**.
CSCwf49390	Device crashes@crypto_map_unlock_map_head.
CSCwe91898	Environmental syslog is not appearing when power cord is disconnected from the redundant PS.

Bug ID	Description
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands.
CSCwh30377	Device data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length.
CSCwf34171	The **configure replace** command fails due to the license udi PID XXX SN:XXXX line on Cisco IOS-XE devices.
CSCwh01425	ITU channel configuration seems not working.
CSCwh20577	Device crashed by TRACK client thread at access invalid memory location.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.
CSCwh36801	Crash in IP input process during tunnel encapsulation.
CSCwh20734	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested and deleted.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwh29805	Custom-app based policy triggering protocol deactivation and CPP traceback with traffic failure.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwf80191	Flowspec on device does not revoke.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config.
CSCwh00332	B2B NAT: when configration ip nat inside/outside on VASI intereface, ack/seq number abnormal.
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.
CSCwf67564	Device observes memory leak at process "SSS Manager".
CSCwf60151	Memory leak with pubd.
CSCwh60190	**ip name-server** command not pushed.
CSCwf56463	IOS process crash during VRRP hash table lookup.
CSCwh11858	Device running IOS-XE crashes when removing FQDN ACL.
CSCwf99906	NTP authentication removed after reload using more than 16 bytes.
CSCwf59173	Segmentation fault at IPv6 BGP backup route notification.
CSCwf67351	Cisco IOx application hosting environment privilege escalation vulnerability.
CSCwf68612	WLC unexpected ueload due to segmentation fault in WNCD process.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.

Bug ID	Description
CSCwf41084	Extranet multicast code improvements for better handling of data structure.
CSCwh04884	VC down due to control-word negotiation.
CSCwf26494	BDI + NTP configuration puts DMI process in degraded mode.
CSCwh96700	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper

Open Bugs - Cisco IOS XE 17.12.2

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

Bug ID	Description
CSCwh73350	Router keeps crashing when processing a firewall feature.
CSCwh94906	WLC segmentation fault crash with Network Mobility Services Protocol (NMSP).
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCwi01046	PoE module is not providing enough power to bring the ports after an unexpected reload.
CSCwh16901	HSEC license installation from the workflow does not complete.
CSCwh77221	SNMP unable to poll Cisco SD-WAN tunnel data after a minute.
CSCwh10813	Renewal of certificates on PKI client fails after a few rollovers.
CSCwh40504	SM-X interface stops passing traffic.
CSCwh79161	Device requires Shut/No Shut to populate IP address from modem to host.
CSCwh57544	Silent reload due to LocalSoftADR causes crash without core file.
CSCwh50510	Router crash with segmentation fault(11), Process = NHRP when processing NHRP traffic.
CSCwh75800	Router unexpectedly reloads while fetching certificate trustpool for SIP TLS.
CSCwh73202	IOS-XE unexpected reboot due to critical process qfp_ucode_utah fault on fp_0_0 (rc=139).
CSCwh73320	NAT pool not working under prefix 16. Available address = zero.
CSCwh96700	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper.
CSCwh45169	Unexpected reboot while dispalying information from cleared SSS session.
CSCwh70449	PMTUD incorrectly converging without attempting to learn a higher MTU.
CSCwf91481	Device crashed unexpectedly after a successful WGB/AP config deployment from OD.

Bug ID	Description
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwh83228	NHRP phase 3 spoke-spoke cache got purged after 5-6 hours with always on traffic running.
CSCwh91136	Cisco IOS XE:Traffic not encrypted and dropped over IPSec SVTI tunnel.
CSCwh96415	Cannot disable DMVPN logging.
CSCwh12093	Enable SoS/ROC feature for DSL.
CSCwf86207	Frame relay DTE router crashes due to EXMEM exhaustion.
CSCwh58252	IPv6 SPD min/max defaulting to values 1 and 2.
CSCwh14083	High CPU due to MPLS MIB poll.
CSCwh22981	WNCD process crashes.
CSCwh99513	VPLS IRB not working when traffic came from VPNv4 and next-hop is learned over VPLS.
CSCwh90851	pubd process showing high CPU utilization.
CSCwh83532	1Gig int on device using GLC-SX-MMD are down/down after changing connection.
CSCwh96891	Memory leak with pubd.
CSCwh91085	Convergence improvement after device reboot with mVPN profile 14.
CSCwh58919	NETCONF: DMI enters degraded mode caused by BGP neighbor configured under the SCOPE command.
CSCuu85298	FIB/LFIB inconsistency after BGP flap.
CSCwf83684	IOS XE router may experience "%FMANRP_QOS-4-MPOLCHECKDETAIL:" errors.
CSCwh59926	EEM is running daily instead of weekly or monthly if special strings @weekly or @monthly are used.
CSCwh24280	Mismatch between the resource allocation and "app-resource profile custom" configuration.
CSCwh82668	Incorrect local MPLS label in CEF after BGP flap.
CSCwh95036	Cisco IOS-XE IPv6 based subscription telemetry does not work.
CSCwh99464	Guestshell connectivity not working with NAT overload.
CSCwh30928	SDA - using "spt-threshold infinity" and having LHR+FHR can cause the S,G to be pruned on the RP.
CSCwh01738	Unexpected reload when using rsh/rcmd.

Bug ID	Description
CSCwh04124	Locally generated traffic received on incorrect interface inbound and dropped by ACL.
CSCwh67285	WLC unable to get telemetry data due to pubd unexpected reload and fail.
CSCwh96332	Device crash due to dhcpd_binding_check.
CSCwh56940	Site tag change wncd working/failing EAP-TLS.
CSCwh44418	ARP incomplete in VRF Mgmt-intf - G0/0/0 - Switch -G0.
CSCwh46559	LLDP location information not sent when configured.
CSCuv36790	**clear bgp** command does not consider AFIs when used with update-group option.
CSCwh02698	Device sending incomplete SGT to ISE.
CSCwh05869	Only portion of HSRP config being pushed via CLI ADDON template.
CSCwf53750	"match pktlen-range" does not work with GRE/IPSEC GRE.
CSCwh60107	In the show tech file, "enable secret" does not get hidden.
CSCwh45579	Unexpected reload on device ucode core @l2_dst_output_goto_output_feature_ext_path.
CSCwh95024	ISIS crash in local uloop.
CSCwh41155	Wrong /32 self, complete map-cache entry for fabric hosts on iBN when overlapping summary exists.
CSCwh31485	Member interface config not applied with mis-match in pcakages.conf files.
CSCwh72437	WLC not sending accounting start for user auth after machine auth on 9105AXW RLAN dot1x port.
CSCwi00680	Router unexpectedly reloads while using DHCP for ISG.
CSCwh96823	IOS-XE router not installing classless-static-routes from DHCP option 121.
CSCwh77706	SVL, 10G link on the active chassis will go down after reload.
CSCwh02592	Device sync fails when device prompt comes along with device banner and TACACS is used.
CSCwh84850	Unexpected reboot in device due to SISF and STP initialization.
CSCwh64903	Crash on device polling SPA sensor data.
CSCwh53432	VLAN name mismatch when authorizing vlan name from radius server and enable vlan fallback.
CSCwh21796	Password getting visible for the mask-secret in show logging.
CSCwh50104	Upgrade failing with config check track-id-name.

Bug ID	Description
CSCwf59929	CTS CORE process crash after configuring role based ACL.
CSCwh81471	IPv6 traffic is passing through when the client is in Webauth Pending state (CWA).
CSCwh93772	Option 121 never requested by IOS-XE client.
CSCwh06087	[IPv6 BGP] multiple sourced paths present for the same prefix.
CSCwh29120	IP SPD queue thresholds are out of range.
CSCwh14953	CBQoS polling for the object cbQosCMPostPolicyBitRate returns incorrect value.
CSCwh89096	Device unexpected reload.
CSCwh99597	After migration MAC/IP only MAC is advertised.
CSCwh75992	"BGP Router" process crash.
CSCwh48058	Memory leak under MallocLite/AAA proxy with NETCONF/RESTCONF.
CSCwh76920	Memory leak in linux_iosd-imag due to SNMP.
CSCwh75112	After a reboot, EAP-FAST/PEAP does not authenticate unless credentials are changed.

Resolved Bugs - Cisco IOS XE 17.12.1a

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

Bug ID	Description
CSCwe57163	Device having **kernel NULL pointer dereference, address: 0000000000000138** kernel panic crash.
CSCwe31226	Issues/discrepancies around CPU alarms generated and sent.
CSCwe82666	Not all HSL entries get pushed if more than 1 HSL entries are configured.
CSCwe43341	TLS control-connections down, traffic from controller dropped with **SdwanImplicitAclDrop**.
CSCwe18124	MACsec remains marked as Secured, but randomly the traffic stops working.
CSCwe18276	Route-map not getting effect when its applied in OMP for BGP routes.
CSCwb74821	Unexpected behavior due to unstable power source.
CSCwe81182	(EPC, packet-trace) for IPsec running COFF (Crypto Offload).
CSCwe63222	Certificate output is not getting changed on renew when Cloud Certificate Authorization is automated.
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
CSCwe90501	Device upgrade fails due to **advertise aggregate** with VRF.

Bug ID	Description
CSCwe85195	AAR: BoW feature ignoring color preference from Tiered Transport preference configuration.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwe06507	Device drops packets with reason 55 (Forus) when port forwarding is enabled from outside to inside.
CSCwd53710	Crash seen when umbrella/zscaler template pushed to device when **name_lookup** takes > 30 sec.
CSCwe66318	NAT entries expire on standby router.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwe70374	Platform punt-policer is not configurable.
CSCwe73408	For some error condition platform_properties may double free.
CSCwd42523	Same label is assigned to different VRFs.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwe57239	All USB internal communcation is closed when using **platform usb disable** command.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write configuration with same crypto value.
CSCwe85421	BFD session down with interface flap.
CSCwe95606	Double GR_Additional log enablement defect.
CSCwe31471	Segmentation fault when per-tunnel QoS configuration withdraw.
CSCwe89404	No way audio when using secure hardware conference with secure endpoints.
CSCwd39257	IOS-XE CPP crash when entering **no ip nat create flow-entries**.
CSCwe70642	AAR overlay actions are applied to DIA traffic.
CSCwa96399	Configuring **entity-information** xpath filter causes syslogs to print, does not return data.
CSCwe79007	Device unexpected reload when doing IPS test with UTD IPS engine.
CSCwe31281	Autotunnel IPsec tracker: Tracker does not come up at all.
CSCwd93401	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM.
CSCwf65696	Non-fabric- load the minimal bootstrap configs again if device rebooted without saving the configurations.

Bug ID	Description
CSCwd76648	Port-channel DPI load-balancing not utilizing all the member-links.
CSCwe39011	GARP on port up/up status from router is not received by remote peer device.
CSCwb39206	Enable VFR CLI.
CSCwe85022	Device is showing 4 additional NR bands support - 1, 3, 7, and 28.

Open Bugs - Cisco IOS XE 17.12.1a

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

Bug ID	Description
CSCwf70854	Changes to speed on the interface via CLI/GUI do not go through unless first done via shell access.
CSCwf72079	Device unexpectedly reloads due to **LocalSoft**.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwh06870	APN password in plain text when device profile is configured.
CSCwf87292	Punt keep alive failure crash on controller-managed device apparently due to data packets.
CSCwf83850	With Pure IPv6, minimal bootstrap unable to onboard Non-Fabric - IPv6 config missing in WAN int G1.
CSCwf94294	Misprograming during vpn-list change under data policy.
CSCwf55145	SFP transceiver DOM not working after some time. However, interface forwards the traffic as expected.
CSCwf94052	BFD going down for newly onboarded device.
CSCwf61720	Device **No licenses in use** after upgrading from traditional to Smart licensing IOS-XE versions.
CSCwf80927	Speed tests to internet from device will fail sometimes.
CSCwf84522	Device unexpected rebooted while classifying packet with CTF (Common Flow Table).
CSCwh00320	**show run** and other show commands not in sync after removing GigabitEthernet3.
CSCwf44703	NAT64 prefix is not originated into OMP.
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands.
CSCwf77252	SIP calls not working on device with ZBFW enabled.
CSCwf96416	Could not access any device show commands at all.
CSCwf67564	Device observes Memory Leak at process **SSS Manager**.

Bug ID	Description
CSCwf34171	**configure replace** command fails due to the license udi **PID XXX SN:XXXX line** on IOS-XE devices.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.
CSCwf69062	SDRA-SSLVPN : The SSLVPN session closes with re-authentication error after some interval of time.
CSCwf79264	Traffic forwarded to wrong VPN. Hence, traffic gets wrong zonepair matched and gets dropped.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwf45486	OMP to BGP redistribution leads to incorrect AS_Path Installation on chosen next-hop.
CSCwh01313	Unexpected reboot due QFP UCode due to IPSec functions.
CSCwf95527	BFD entries removed.
CSCwe26895	Router has LocalSoftADR crash, writes flat core, and reloads.
CSCwh01318	Multiple crashes observed on platform due to memory exhaustion.
CSCwf71116	Static route keep advertising via OMP even though there is no route.
CSCwf60120	Static NAT entry gets deleted from running configuration, but remains in startup configuration.
CSCwh00332	B2B NAT: when configration ip nat inside/outside on VASI intereface, ack/seq number abnormal.
CSCwf78735	Device uses the NIM-1T/4T card for interconnection, and NAT+ GRE over IPsec cannot be applied.
CSCwf84960	C-NIM-2T: LED L remains green after port shutdown.
CSCwf49390	Device crashes@crypto_map_unlock_map_head.
CSCwh67812	Unable to configure crypto map on a physical interface due to which crypto map-based VPN's cannot be formed.

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

- End-of-Sale and End-of-Life Announcement
- 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 DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.