Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE Dublin 17.12.x

First Published: 2023-08-22

Last Modified: 2024-08-16

Full Cisco Trademarks with Software License

About Cisco 1000 Series Integrated Services Routers

The Cisco 1000 Series Integrated Services Routers (also referred to as router in this document) are powerful fixed branch routers based on the Cisco IOS XE operating system. They are multi-core routers with separate core for data plane and control plane. There are two primary models with 8 LAN ports and 4 LAN ports. Features such as Smart Licensing, VDSL2 and ADSL2/2+, 802.11ac with Wave 2, 4G LTE-Advanced and 3G/4G LTE and LTEA Omnidirectional Dipole Antenna (LTE-ANTM-SMA-D) are supported on the router.

Note Cisco IOS XE Dublin 17.12.1a is the first release for Cisco 1000 Series Integrated Services Routers in the Cisco IOS XE Dublin 17.12.x release series.

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.

New and Changed Hardware and Software Features

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 1: 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 2: New Software Features

Feature	Description
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.
Profile Clean-up on LTE Modems Using Factory Reset Button	To clean the cellular modem completely, users can press the physical factory-reset button on the device, which enables the inbuilt **lte cellular-profile-cleanup** command to erase the configuration setup and profiles. This command is disabled by default, but can be enabled only when the factory-reset button is pressed.
Quantum-Safe Encryption Using Post-Quantum Preshared Keys	This enhancement introduces support for Quantum-Safe Encryption using Post-Quantum Preshared Keys for the following platforms: • Cisco 1000 Series Integrated Services Routers • Cisco Catalyst 8500 Series Edge Platforms

Feature	Description
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.
TrustSec and Software-Defined Access Scale Measurement	With this feature, the scale numbers for TrustSec and Software-Defined Access (SDA) are measured for the following: • Security Group Tag (SGT) or Destination Group Tag (DGT) Policies • Unidirectional IPv4 SGT Exchange Protocol (SXP) connections • Bidirectional IPv4 SXP connections • IPv4 SGT Bindings • IPv6 SGT Bindings • Security Group Access Control Entries (SG ACEs)
Cube Features	
CUBE/LGW: 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.

Note From Cisco IOS XE Release 17.9.1a, guestshell is removed from the IOS XE software image. As a result, Zero Touch Provisioning (ZTP) python script is no longer supported on Cisco 1000 Series Integrated Services Routers. If you need to use guestshell, then download it from https://developer.cisco.com/docs/iox/#!iox-resource-downloads/downloads. For more information, see Guestshell installation procedure.

Cisco ISR1000 ROMmon Compatibility Matrix

The following table lists the ROMmon releases supported in Cisco IOS XE 16.x.x releases and Cisco IOS XE 17.x.x releases.

Note To identify the manufacturing date, use the **show license udi** command. For example:

```
Router#show license udi
UDI: PID:C1131-8PLTEPWB,SN:FGLxxxxLCQ6
```

The xxxx in the command output represents the manufacturing date.

- If the manufacturing date is greater than or equal to 0x2535, the manufactured ROMmon version is 17.6(1r) or higher.
- If the manufacturing date is less than 0x2535, the ROMmon will be automatically upgraded to 17.5(1r) or above when the Cisco IOS XE 17.9.x release is installed.
- The minimal or recommended ROMmon version for devices using Cisco IOS XE 17.5 or later is 17.5(1r) or later.

Note To upgrade to Cisco IOS XE Dublin 17.12.x, follow these steps:

1. If you are on a device that is running software version between Cisco IOS XE 16.x to Cisco IOS XE 17.4.x, upgrade to any IOS XE image between Cisco IOS XE 17.5.x to Cisco IOS XE 17.10.x.
2. After performing step a, upgrade to Cisco IOS XE 17.12.x.
3. For devices that are running on software version Cisco IOS XE 17.5.x or later, you can upgrade to Cisco IOS XE 17.12.x directly.

Table 3: Minimum and Recommended ROMmon Releases Supported on Cisco 1000 Series Integrated Services Routers

Cisco IOS XE Release	Minimum ROMmon Release for IOS XE	Recommended ROMmon Release for IOS XE
16.6.x	16.6(1r)	16.6(1r)
16.7.x	16.6(1r)	16.6(1r)
16.8.x	16.8(1r)	16.8(1r)
16.9.x	16.9(1r)	16.9(1r)
16.10.x	16.9(1r)	16.9(1r)
16.11.x	16.9(1r)	16.9(1r)
16.12.x	16.9(1r)	16.12(1r)
17.2.x	16.9(1r)	16.12(1r)
17.3.x	16.12(2r)	16.12(2r)
17.4.x	16.12(2r)	16.12(2r)

Cisco IOS XE Release	Minimum ROMmon Release for IOS XE	Recommended ROMmon Release for IOS XE
17.5.x	17.5(1r)	17.5(1r)
17.6.x	17.5(1r)	17.5(1r)
17.7.x	17.5(1r)	17.5(1r)
17.8.x	17.5(1r)	17.5(1r)
17.9.x	17.5(1r)	17.5(1r)
17.10.x	17.5(1r)	17.5(1r)
17.11.x	17.5(1r)	17.5(1r)
17.12.x	17.5(1r)	17.5(1r)

Resolved and Open Bugs in Cisco IOS XE 17.12.x

Resolved Bugs in Cisco IOS XE 17.12.4

Table 4: Resolved Bugs in Cisco IOS XE 17.12.4

Bug ID	Description
CSCwj70335	Crypto IKEv2 - Fragmented authentication packets detected as malformed on 3rd party vendor device.
CSCwj44868	GETVPN COOP KS | Wrong Severity for Rekey Acknowledgement configuration mismatch log message
CSCwi88969	FMFP-3-OBJ_DWNLD_TO_DP_FAILED observed when delete and configure zone-pair back
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
CSCwj45130	Segmentation Fault - Process = IPSec dummy packet process

Bug ID	Description
CSCwj88872	IPSec tunnel fails to establish due to error IPSec policy invalidated proposal
CSCwj73113	MGCP GW doesn't 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
CSCwi84767	Memory dump outputs appear without debugs enabled in SSL VPN code
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 cpp ucode on the router.
CSCwh86053	ENH: Config Parser Issue for NAT with Extendable and Redundancy
CSCwj42249	Disabling PMTU-Discovery with MTU Change and BFD Flap Breaks Packet Duplication
CSCwh16595	Flex: Peer failed to up after shut/noshut L2 port with SFP inserted and switchport mode configured
CSCwi78365	Trim installed certificate on upgrade
CSCwj72888	Reload in tcp_sanity due to l4 pointer not set
CSCwi93784	(SWI case 01257768)FW upgrade does not work properly on P-LTE-MNA with 17.12.1a and 17.12.2 IOS
CSCwj33292	AnyConnect connection trough IPSec fails when connecting from an RDP user to an IOS/IOS-XE headend
CSCwi60071	ipv6 PREFIX delegation is not working on ADSL PPPOA
CSCwj06622	segmentation fault and core files are seen on IOS-XE in controller-manged SD-WAN due to speedtest
CSCwi16111	ipv6 tcp adjust-mss not working after delete and reconfigure
CSCwj29947	AAA authorization failure during IKEv2 phase negotiation caused unexpected reboot
CSCwj25619	ISR1K 17.12.2 Auto-negotiation fails to endpoint hardcoding 10/half
CSCwf87975	Router crashed when port-channel interface flap with scale of per-tunnel QoS policies.

Open Bugs in Cisco IOS XE 17.12.4

Table 5: Open Bugs in Cisco IOS XE 17.12.4

Bug ID	Description
CSCwj79987	C1121X SD-WAN Router does not establish BFD sessions after upgrade to 17.9.3a or 17.9.4a
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
CSCwk42493	Cellular interface in last-resort mode should be admin up, line protocol down
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration
CSCwj06950	C1117 - DSL module gets stuck in a booting state
CSCwk58303	Watchdog crash during IPv6 cef adjacency routines
CSCwk63722	Startup Configuration Failure Post PKI Server Enablement
CSCwj77594	IOS XE Controller Mode - WAN IP is allowed to be configured as SYSTEM IP
CSCwk54544	SD-WAN ZBFW TCAM misprogramming after rules are reordered on c8300
CSCwb47658	Repeated and endless messages "Network change event - activated 4G Carrier Aggregation."
CSCwj90614	High CPU utilisation for confd_cli
CSCwk03686	Crash due a segmentation fault due a negative value
CSCwi96692	**** Unable to Install HSEC K9 Licence for PID C1111-8PLTELAWF & C1111X-8P ****
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwh45389	C9800: Key manager crash after hostname change with usage keys
CSCwk12524	Device reloaded due to ezManage mobile app Service.
CSCwk65071	Unexpected reboot due to IOSXE-WATCHDOG DBAL EVENTS after Cellular interface flap
CSCwf91481	Device crashed unexpectedly after a successful WGB/AP config deployment from OD.
CSCwk52677	C1118-8P / DSL router crashing due to %PLATFORM-3-ELEMENT_CRITICAL memory level / iomd process
CSCwi96187	P-5GS6-GL FN980 modem fW upgrade is failing.
CSCwh91136	IOS XE:Traffic not encrypted and droped over IPSEC SVTI tunnel

Bug ID	Description
CSCwj23674	Dialer interface MAX MTU for PPPOA is 1492
CSCwj84949	Unencrypted Traffic Due to Non-Functional IPsec Tunnel in FLEXVPN Hub & Spoke Setup
CSCwk20995	PPPoE session with sub-interface getting stuck after reboot
CSCwk30527	IKEv2 session is down after reload if identity local address is assigned to interface on Switch
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.
CSCwi31110	Traceback seen @_nhrp_cache_delete due to negative global cache count.

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 in Cisco IOS XE 17.12.3

Table 6: Resolved Bugs in Cisco IOS XE 17.12.3

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 is not working.
CSCwh77221	SNMP unable to poll tunnel data after a minute.
CSCwh96578	SKA_PUBKEY_DB leak in TDL.
CSCwh69765	Security policy w/IPS external syslog config failing generation for specific models.
CSCwh87619	ZBFW is unable to detect packets on TenGig interface.
CSCwi06843	Endpoint tracker triggers a CPU hog.
CSCwh80441	Cosmetic 3G issue causing distress to customers - modem WCDMA 900 is displayed as unknown.

Bug ID	Description
CSCwh10813	Add verbose log to indicate grant ra-auto to undo configuring the grant auto in PKI server.
CSCwi60312	Device does not boot up in full configuration.
CSCwh93257	Device creates crooked NAT entry if 2 or more IP phones from NAT outside register to the same server.
CSCwi59121	Mobile-app causing excessive authorization attempts with a null username.
CSCwi08171	Router may crash due to crypto IKMP process.
CSCwi49231	Device audio loss for 4 seconds.
CSCwi06404	PKI crash after failing a CRL fetch.
CSCwh50510	Router unexpectedly reloads during Trustpool retrieval for SIP TLS certificate.
CSCwh75800	Router unexpectedly reloads while fetching certificate Trustpool for SIP TLS.
CSCwi28781	EPBR generates error when the policy is added and deleted multiple times.
CSCwh45169	Unexpected reboot while dispalying information from cleared SSS session.
CSCwh70449	PMTUD incorrectly converging without attempting to learn a higher MTU.
CSCwh96415	Cannot disable the 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.
CSCwi51326	CPP CP SVR crash after decoding all packets to text (using l2 copy) on FIA trace.
CSCwi76087	ATO: Session fails to come up when the tunnel is repeatedly shut and no shut in a loop (similar to customer unplugging and plugging in a cable).
CSCwi55379	IPsec traffic is being dropped on strongswan when PPK is implemented.
CSCwi63042	Packet drops observe between LISP EID over GRE tunnel.
CSCwi79584	Upgrade failure for a routing device through the management system due to a modified system configuration.
CSCwi30529	AAA: Template push fail when AAA authorization is set to local.

Open Bugs in Cisco IOS XE 17.12.3

Table 7: Open Bugs in Cisco IOS XE 17.12.3

Bug ID	Description
CSCwi03502	Create CLI to push at#enadis=0 followed with at#reboot to FN980 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 in Cisco IOS XE 17.12.2

Table 8: Resolved Bugs in Cisco IOS XE 17.12.2

Bug ID	Description
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.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot.
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.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwf82676	CPU usage mismatch in **show sdwan system status** vs **show proc cpu platform**.
CSCwf49390	crashes@crypto_map_unlock_map_head.
CSCwe91898	Environmental syslog is not appearing when power cord is disconnected from the redundant PS.
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands.

Bug ID	Description
CSCwh44986	Device to host C1117-4PLTE loopback unreachable.
CSCwh30377	Data plane crash in Umbrella/OpenDNS processing due to incorrect UDP length.
CSCwf34171	**configure replace** command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwh20734	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested and deleted.
CSCwh01425	ITU channel configuration seems not working on device.
CSCwh20577	Crashed by TRACK client thread at access invalid memory location.
CSCwh00963	Unable to migrate from ADSL to VDSL without reboot on C1117-4PLTEEA.
CSCwh36801	Crash in IP Input process during tunnel encapsulation.
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error.
CSCwd39219	SMS archive does not work when ftp transaction is of VRF.
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 will 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.
CSCwh08948	Show platform hardware throughput crypto/ambiguous outputs.
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.
CSCwh96700	Carrier Grade NAT reaching max host entries and failing to translate due to gatekeeper

Open Bugs in Cisco IOS XE 17.12.2

Table 9: Open Bugs in Cisco IOS XE 17.12.2

Bug ID	Description
CSCwh58252	IPv6 SPD min/max defaulting to values 1 and 2.
CSCwh14083	High CPU due to MPLS MIB poll.
CSCwh22981	WNCD process crashes.

Bug ID	Description
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.
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.

Bug ID	Description
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.
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.

Bug ID	Description
CSCwh76920	Memory leak in linux_iosd-imag due to SNMP.
CSCwh75112	After a reboot, EAP-FAST/PEAP does not authenticate unless credentials are changed.
CSCwh73350	Device 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 SDWAN tunnel data after a minute.
CSCwh10813	Add verbose log to indicate grant ra-auto un configures grant auto in PKI server.
CSCwh79161	WP7607 Requires shut/no shut to populate IP address from modem to host.
CSCwh57544	Silent reload due to LocalSoftADR causes crash without core file.
CSCwh50510	Device crash with segmentation fault(11), Process = NHRP when processing NHRP traffic.
CSCwh75800	CUBE router unexpectedly reloads while fetching certificate Trustpool for SIP TLS.
CSCwh73320	NAT pool does 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.
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	IOS XE: Traffic not encrypted and droped over IPSEC SVTI tunnel.
CSCwh96415	Cannot disable DMVPN logging in.
CSCwh12093	Enable SoS/ROC feature for DSL.
CSCwf86207	Frame relay DTE router crashes due to EXMEM exhaustion.

Resolved Bugs in Cisco IOS XE 17.12.1a

Table 10: Resolved Bugs in Cisco IOS XE 17.12.1a

Bug ID	Description
CSCwe82666	Not all HSL entries get pushed to device if more than 1 HSL entries are configured via vManage.
CSCwe31226	Issues/discrepancies around CPU alarms generated and sent to vManage from cEdge.
CSCwe43341	TLS control-connections down, traffic from controller dropped with SDWAN implicit ACL drop.
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.
CSCwf83850	With Pure IPv6, minimal bootstrap unable to onboard Non-Fabric - ipv6 config missing in wan int G1.
CSCwb74821	Unexpected behavior due to unstable power source.
CSCwe81182	(EPC, packet-trace) for IPsec running COFF (Crypto OFFLOAD).
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
CSCwe90501	Upgrade fails due to advertise aggregate with vrf.
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.
CSCwd53710	Crash seen when umbrella/zscaler template pushed to device when name_lookup takes 30 sec.
CSCwe66318	NAT entries expire on standby router.
CSCwf83985	With pure IPv6 overlay, vbond vpn 0 ge0/0 interface if-oper-status down after power off/on.
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwe70374	Device 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 communication is closed when using **platform usb disable** command.

Bug ID	Description
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwe85421	cEdge BFD session down with interface flap.
CSCwe83169	Pseudowire control word not working on device.
CSCwe95606	Double GR_Additional log enablement defect.
CSCwe31471	Segmentation fault in SDWAN PB rx when per-tunnel qos config 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**.
CSCwe63222	Certificate output is not getting changed on renew when cloud certificate authorization is automated.
CSCwe70642	AAR overlay actions are applied to DIA traffic.
CSCwa96399	Configuring entity-information xpath filter causes syslogs to print, does not return data.
CSCwe79007	cEdge unexpected reload when doing ips test with UTD ips engine.
CSCwe31281	Autotunnel IPsec tracker: Tracker does not come up at all on vEdge.
CSCwd93401	AppNav-XE: Policy-map edit on cluster with multiple service context fails to program TCAM.
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 in sdwan mode.
CSCwe85022	Telstra Cert: FN980 modem is showing 4 additional NR bands support - 1, 3, 7, and 28.

Open Bugs in Cisco IOS XE 17.12.1a

Table 11: Open Bugs in Cisco IOS XE 17.12.1a

Bug ID	Description
CSCwf70854	Changes to speed on the interface via CLI/GUI does 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 cellular controller profile is configured.

Bug ID	Description
CSCwf87292	Punt keep alive failure crash on device controller managed apparently due to for us 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	No licenses in use after upgrading from traditional to Smart Licensing IOS-XE versions.
CSCwf80927	Speed tests to internet from device triggered.
CSCwf84522	Unexpected rebooted while classifying packet with CTF (Common Flow Table).
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	Can not access any **show sdwan** commands at all.
CSCwf67564	Device observes Memory Leak at process SSS Manager.
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 SSL VPN 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 Local Soft ADR 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.

Bug ID	Description
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config
CSCwh00332	B2B NAT: when configuration **ip nat inside/outside** on VASI intereface, ack/seq number abnormal.
CSCwf49390	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 Information

- Hardware Installation Guide
- Software Configuration Guide
- Smart Licensing using Policy

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.