Release Notes for Cisco 1100 Terminal Services Gateway

First Published: 2020-05-12

Last Modified: 2024-10-18

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

About Cisco 1100 Terminal Services Gateway

Cisco 1100 Terminal Services Gateway are terminal servers that provides asynchronous connections to the console ports for Cisco devices.

Table 1: Base Models of the Cisco 1100 Terminal Services Gateway

Base Models	Asynchronous Ports	NIM Slot	Switch	Memory
C1100TG-1N32A	32	Yes	None	2GB Dram/ 4GB flash
C1100TG-1N24P32A	32	Yes	24 port L2 Switch	4GB Dram/ 4GB flash
C1100TGX-1N24P32A	32	Yes	24 port L2 Switch	8GB Dram/ 8GB flash

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

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

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

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 Enhanced Hardware and Software Features

New and Changed Hardware Features

Table 2: New Hardware Features

Feature	Description
Cisco 1100 Terminal Services Gateway	The Cisco 1100 Terminal Services Gateway are based on Cisco IOS XE Amsterdam 17.2 release, multi-core data plane and 4 core CPU. The Cisco 1100 Terminal Services Gateway are in two platform series. The base model has a 32 async ports with 2 GB memory, the plus model has 32 ports, 24 L2 switch and 4GB or 8GB memory to support programmability features. A 16 port async ports daughter card is available to extend onboard async ports to 48 for both these platforms.

New and Changed Software Features

New and Changed Software Features in Cisco IOS XE 17.14.1a

Table 3: New Software Features

Feature	Description
NIM-VAB-A Support	From Cisco IOS XE 17.14.1a, this feature extends NIM-VAB-A support to Cisco 1100 Terminal Services Gateway. NIM-VAB-A is a Cisco Multimode VDSL2 and ADSL2/2+ NIM that provides single-port multimode VDSL2 and ADSL2/2+ WAN connectivity.

New and Changed Software Features in Cisco IOS XE 17.13.1a

Table 4: New Software Features

Feature	Description
Proxy Mobile IPv6 Support for MAG Functionality.	From Cisco IOS XE 17.13.1a, Mobile Access Gateway (MAG) support has been enabled on C1100 Terminal Gateway platform.
Support for Security-Enhanced Linux	SELinux (Security-Enhanced Linux) is a solution designed to incorporate a strong, flexible mandatory access control (MAC) architecture into Cisco IOS XE platforms. From Cisco IOS XE 17.13.1a, SELinux is enabled by default in Enforcing mode for Cisco IOS XE platforms.

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 5: 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 6: New Software Features

Feature	Description
Support for C-NIM-2T on C1100TGX-1N24P32A	This feature extends C-NIM-2T support to C1100TGX-1N24P32A of the Cisco 1100 Series Terminal Services Gateway. C-NIM-2T is a dual combo port module with two RJ-45 copper line ports and two SFP fiber ports. This NIM module supports MACsec 128/256-bit encryption.

New and Changed Software Features in Cisco IOS XE 17.9.5a

There are no new features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.4a

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 17.9.1a

Table 7: New Software Features

Feature	Description
New mechanism to send data privacy related information	A new mechanism to send data privacy related information was introduced. This information is no longer included in a RUM report. If data privacy is disabled (**no license smart privacy**{**all**|**hostname**|**version**} command in global configuration mode), data privacy related information is sent in a separate sync message or offline file. Depending on the topology you have implemented, the product instance initiates the sending of this information in a separate message, or CSLU and SSM On-Prem initiates the retrieval of this information from the product instance, or this information is saved in an offline file. For more information, see license smart (global config).
Hostname support	Support for sending hostname information was introduced. If you configure a hostname on the product instance and disable the corresponding privacy setting (**no license smart privacy hostname** command in global configuration mode), hostname information is sent from the product instance, in a separate sync message or offline file. Depending on the topology you have implemented, the hostname information is received by CSSM, CSLU, and SSM On-Prem. It is then displayed on the corresponding user interface. For more information, see license smart (global config). With the introduction of this enhancement, the hostname limitation which existed from Cisco IOS XE Amsterdam 17.3.2 to Cisco IOS XE Cupertino 17.8.x – is removed. In these earlier releases, hostname information is not sent or displayed on various licensing utilities (CSSM, CSLU, and SSM On-Prem).

Feature	Description
RUM Report Throttling	For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down that was caused by an excessive generation of RUM reports. You can override the reporting frequency throttling, by entering the **license smart sync** command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases.
Virtual Routing and Forwarding (VRF) Support	On a product instance where VRF is supported, you can configure the **license smart vrf** *vrf_string* command and use a VRF to send licensing data to CSSM, or CSLU, or SSM On-Prem. For more information, see license smart (global config) **Note** When using a VRF, the supported transport types are **smart** and **cslu** only.

New and Changed Software Features in Cisco IOS XE 17.8.1a

Table 8: New Software Features

Feature	Description
Booster Performance license	The Booster Performance license enables unthrottled throughput (for unencrypted traffic). Without it, throughput for unencrypted traffic is restricted to 500 Mbps. To enable the license, enter the **platform hardware throughput level boost** command in global configuration mode.
Support for X.25 protocol on Cisco 1100 Terminal Services Gateway	The X.25 protocol is now supported on Cisco 1100 Terminal Services Gateway. X.25 is the ITU-T standard that defines connections maintained between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for remote terminal access and computer communications.

New and Changed Software Features in Cisco IOS XE 17.6.8a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.6.6a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see the Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

New and Changed Software Features in Cisco IOS XE 17.6.5a

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 17.4.1

Table 9: New Software Features

Feature	Description
Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy:	SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM. Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. The product instance can be configured to *push*the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to *pull* the required information from a product instance at a configurable frequency. After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Offline and online options are available for synchronization between CSSM and SSM On-Prem. • Minimum Required SSM On-Prem Version: Version 8, Release 202102 • Minimum Required Cisco IOS XE Version: Cisco IOS XE Amsterdam 17.3.3. (If a product was first introduced in a later release, that release becomes the minimum required IOS-XE version for the product.)
Support for Synchronous Serial NIMs	From Cisco IOS XE Bengaluru 17.4.1, the following Synchronous Serial NIMs are supported on Cisco 1100 Series Terminal Services Gateway: • Cisco 1-Port Serial WAN Network Interface Card (NIM-1T) • Cisco 2-Port Serial WAN Network Interface Card (NIM-2T) • Cisco 4-Port Serial WAN Network Interface Card (NIM-4T)

Feature	Description
Support for Cisco T1/E1 NIM	This feature extends support for the following Cisco T1/E1 NIM modules in data mode: • NIM-1MFT-T1/E1 • NIM-2MFT-T1/E1 • NIM-4MFT-T1/E1 • NIM-8MFT-T1/E1 • NIM-1CE1T1-PRI • NIM-2CE1T1-PRI • NIM-8CE1T1-PRI The Cisco T1/E1 NIM module does not support TDM subdivision and analog services.
Support for Smart Licensing	Cisco DNA Center supports Smart Licensing Using Policy functionality starting with Cisco DNA Center Release 2.2.2. The corresponding minimum required Cisco IOS XE Release for this platform is Cisco IOS XE Bengaluru 17.4.1. Implement the "Connected to CSSM Through a Controller" topology to have Cisco DNA Center manage a product instance. When you do, the product instance records license usage, but it is the Cisco DNA Center that initiates communication with the product instance to retrieve and report usage to Cisco Smart Software Manager (CSSM), and returns the acknowledgement (RUM ACK). In order to meet reporting requirements, Cisco DNA Center provides ad hoc or on-demand reporting, as well as scheduled reporting options. **Note** Cisco DNA Center also provides workflows for the installation and removal of the Smart Licensing Authorization Code (SLAC) for a product instance, if applicable. On the Cisco DNA Center GUI, you can generate a SLAC *only* for HSECK9 licenses, and *only* for certain product instances. See the configuration guide for details.

New and Changed Software Features in Cisco IOS XE 17.3.8a

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 17.3.8

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.7

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.6

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.5

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.4

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.3

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.3.2

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.2

The following are the new features in Cisco 1100 Terminal Services Gateway in the 17.2 release:

- IPv4 & IPv6 forwarding
- IP Routing (OSPF, EIGRP, BGP)
- IP/GRE tunneling, IPv4-to-IPv6 tunneling
- VRF lite
- PBR
- MPLS
- Multicast
- Flexible Netflow
- QoS/MQC
- NBAR
- Routed IEEE 802.1q VLANs
- FHRPs (VRRP/HSRP/GLBP)
- HQoS
- RADIUS, TACACS+, AAA

The following are the new security features in Cisco 1100 Terminal Services Gateway in the 17.2 release:

- ACL (L3/L4)
- FW (L4/L7)
- NAT
- IPSec

- DMVPN
- Router security – Akido secure boot, Code Signing, and CSL

Resolved and Open Bugs

Resolved Bugs in Cisco IOS XE 17.15.1a

Table 10: Resolved Bugs in Cisco IOS XE 17.15.1a

Bug ID	Description
CSCwj51700	CPP crashes after re-configuring "ip nat settings pap limit ... bpa" feature in high QFP state.
CSCwk33173	EzPM application-performance profile cause memory leak and crash with long-lived idle TCP flows.
CSCwk45165	fman_fp Memory Leak on router.
CSCwj84949	Unencrypted Traffic Due to Non-Functional IPsec Tunnel in FLEXVPN Hub & Spoke Setup.
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwk12524	Device reloaded due to ezManage mobile app Service.
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration.
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.
CSCwk59367	IOX helper files missing in the routing platform.

Open Bugs in Cisco IOS XE 17.15.1a

Table 11: Open Bugs in Cisco IOS XE 17.15.1a

Bug ID	Description
CSCwk49806	Router running IOS 17.06.05 rebooted unexpectedly due to process NHRP crash.
CSCwi87546	Unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released.
CSCwk61238	RRI static not populating route after reload if stateful IPSec is configured.
CSCwk98578	GETVPN IPv6 crypto map not shown in interface configuration.
CSCwk70630	17.12.02 Cannot import device certificate.
CSCwk81360	Cisco IOS-XE Router can reboot unexpectedly while configuring NAT Static Translation.

Bug ID	Description
CSCwk63722	Startup Configuration Failure Post PKI Server Enablement.
CSCwk90014	NAT DIA traffic getting dropped due to port allocation failure.
CSCwm12851	IOS-XE 17.12.3 uses 3DES as default rekey algorithm for GETVPN.

Resolved Bugs in Cisco IOS XE 17.14.1a

Table 12: Resolved Bugs in Cisco IOS XE 17.14.1a

Bug ID	Description
CSCwh94906	Device segmentation fault crash with Network Mobility Services Protocol (NMSP) .
CSCwi61369	Router may unexpectedly reload due to SIGABRT.
CSCwi40603	Memory leak in the Crypto IKMP process .
CSCwb25507	CWMP : Add vendor specific parameter for NBAR protocol pack version.
CSCwi82548	Crash in IKEv2 Cluster Load Balancer.
CSCwi85293	IKEv2 IPv6 Cluster Load balance: Secondary in cluster unable to connect to cluster in case of FVRF.
CSCwi16111	IPv6 tcp adjust-mss not working after delete and reconfigure.

Open Bugs in Cisco IOS XE 17.14.1a

Table 13: Open Bugs in Cisco IOS XE 17.14.1a

Bug ID	Description
CSCwj09284	Unexpected reboot in WLC due to SSL.
CSCwj48393	ISG: Service with no priority are not working as expected.
CSCwj48421	%CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi.
CSCwj43905	Unexpected Reboot Due to QFP-Ucode-Radium Failure.
CSCwj34578	NAT46 translations are dropped when NAT64 router is also Carrier Supporting Carrier CE.
CSCwj30334	CVLA ucode crash when attempting merge on used block.
CSCwj13681	Device can only store 64 FQDN patterns, but config accepts more than 64.

Resolved Bugs in Cisco IOS XE 17.13.1a

Table 14: Resolved Bugs in Cisco IOS XE 17.13.1a

Bug ID	Description
CSCwh10813	Add verbose log to indicate grant ra-auto un configures grant auto in PKI server.
CSCwf25735	Device QoS more than four remark with set-cos not work.
CSCwf14607	Crash observed exporting PKCS12 to terminal via SSH CLI.

Open Bugs in Cisco IOS XE 17.13.1a

Table 15: Open Bugs in Cisco IOS XE 17.13.1a

Bug ID	Description
CSCwh94906	Router WLC segmentation fault crash with Network Mobility Services Protocol (NMSP).
CSCwi00369	Device lost security parameter after upgrade.
CSCwi06843	Endpoint tracker triggers a CPU Hog.
CSCwi16015	[SIT]: SSE tunnels don't come up with Dialer interface.Relax check in IKE.
CSCwi13563	IP SLA probe for End-point-tracker doesnt work once endpoint tracker is changed until reload.
CSCwi06404	Router PKI related crash after failing a CRL Fetch.
CSCwi14178	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed.
CSCwi23562	When RADIUS down, and there is an IKE-AUTH request received, the box stops replying to DPD packets.
CSCwh65016	Unexpected Reboots on Cedge Due to QFP Exception.
CSCwi08171	Router may crash due to Crypto IKMP Process.
CSCwi05395	SNMP bulkget cannot get loss, latency and jitter for Probe Class Table & Class Interval Table OIDs
CSCwh84068	Router crash after changing NAT HSL configuration.
CSCwi15688	Unexpected NAT translation occurs in a specific network.
CSCwi19875	Decice is unable to process hidden characters in a file while trying to use bootstrap method.
CSCwh91136	IOS XE: Traffic not encrypted and droped over IPSEC SVTI tunnel.

Bug ID	Description
CSCwi11807	SNMP bulk get breaks the OID 'appRouteStatisticsTable' after minute Not returning the correct order.
CSCwi35177	Router crash caused by continuous interface flap, interface associated to many ipsec interfaces.
CSCwi30529	AAA: Template push fail when aaa authorization is set to local.
CSCwh52440	IP SLA doesnt have checks for ICMP probes to be sent on source interface.

Resolved Bugs in Cisco IOS XE 17.12.4

Table 16: Resolved Bugs in Cisco IOS XE 17.12.4

Bug ID	Description
CSCwh86053	ENH: Config Parser Issue for NAT with Extendable and Redundancy.
CSCwj38106	Only one split-exclude subnet is pushed to client PC with IOS-XE headend for a RA VPN connection.
CSCwj36915	Device macsec not working under LACP port-channel member port.
CSCwj45130	Segmentation Fault - Process = IPSec dummy packet process.
CSCwi68865	Memory leak in Crypto IKEv2 due to C_NewObject.
CSCwj09284	Unexpected reboot in WLC due to SSL.
CSCwj88872	IPsec tunnel fails to establish due to error IPSec policy invalidated proposal.
CSCwh01095	Rapid memory leak on "ngiolite" process.
CSCwj70335	Crypto IKEv2 - Fragmented Authentication packets detected as malformed on 3rd party vendor device
CSCwj33292	AnyConnect connection trough IPSec fails when connecting from an RDP user to an IOS/IOS-XE headend.
CSCwj44868	GETVPN COOP KS | Wrong Severity for Rekey Acknowledgement configuration mismatch log message.
CSCwi40603	Memory leak in the Crypto IKMP process .
CSCwh73320	NAT Pool doesn't working under prefix 16. Available address = zero.
CSCwi82405	mGRE Tunnels with shared ipsec profile cause ucode crash.
CSCwi16111	IPv6 tcp adjust-mss not working after delete and reconfigure.
CSCwj29947	AAA authorization failure during IKEv2 phase negotiation caused unexpected reboot.
CSCwj72888	Reload in tcp_sanity due to l4 pointer not set.

Bug ID	Description
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.
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 17: Open Bugs in Cisco IOS XE 17.12.4

Bug ID	Description
CSCwk31560	NAT Command not readable after reloaded.
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.
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration.
CSCwk63722	Startup Configuration Failure Post PKI Server Enablement.
CSCwk58303	Watchdog crash during IPv6 cef adjacency routines.
CSCwf91481	IR1835 crashed unexpectedly after a successful WGB/AP config deployment from OD.
CSCwk30527	IKEv2 session is down after reload if identity local address is assigned to interface on Switch.
CSCwj84949	Unencrypted Traffic Due to Non-Functional IPsec Tunnel in FLEXVPN Hub & Spoke Setup.
CSCwh91136	IOS XE:Traffic not encrypted and droped over IPSEC SVTI tunnel .
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 in Cisco IOS XE 17.12.3

Table 18: Resolved Bugs in Cisco IOS XE 17.12.3

Bug ID	Description
CSCwh73350	Router keeps crashing when processing a firewall feature.

Bug ID	Description
CSCwi08171	Router may crash due to Crypto IKMP Process.
CSCwi06404	PKI crash after failing a CRL Fetch.
CSCwh50628	Race condition crash on IOS-XE device.
CSCwh18120	IKEv2 - diagnose feature is taking 11% CPU during session bring up.
CSCwh10813	Add verbose log to indicate grant ra-auto un configures grant auto in PKI server.
CSCwh50510	Router Crash with Segmentation fault (11), Process = NHRP when processing NHRP traffic.
CSCwi28227	Router / IOS XE 17 / NAT HSL logging vrf-filter not working.
CSCwf86207	Frame Relay DTE router crashes due to EXMEM exhaustion.
CSCwi25737	Router should discard IKE Notification messages with incorrect DOI.
CSCwi55379	IPsec Traffic is being dropped on Strongswan when PPK is implemented.
CSCwh45169	Unexpected Reboot while Dispalying Information from Cleared SSS Session.
CSCwh93257	Router creates crooked NAT entry if 2 or more ip phone from nat outside register to same server.
CSCwi59121	Device: Mobile-app causing excessive Authorization attempts with a Null Username.
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCwi63042	Packet drops observe between LISP EID over GRE Tunnel.
CSCwh96578	SKA_PUBKEY_DB leak in TDL.
CSCwi76087	ATO : Session fails to come up with Tunnel its shut no shut in loop (cable unplug-plug in customer).
CSCwh96415	Can't disable DMVPN logging in IOS-XE 17.8 and higher.

Open Bugs in Cisco IOS XE 17.12.3

Table 19: Open Bugs in Cisco IOS XE 17.12.3

Bug ID	Description
CSCwj08744	Unexpected reload when using "show running-config full | format".
CSCwi46997	NAT Command not readable after reloaded.
CSCwi16111	IPv6 tcp adjust-mss not working after delete and reconfigure.

Resolved Bugs in Cisco IOS XE 17.12.2

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

Table 20: Resolved Bugs in Cisco IOS XE 17.12.2

Bug ID	Description
CSCwf67564	Device observes memory leak at process "SSS Manager".
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.
CSCwf41084	Extranet multicast code improvements for better handling of data structure.
CSCwh04884	VC down due to control-word negotiation.
CSCwf84960	C-NIM-2T: LED L remains green after port shutdown.
CSCwf49390	crashes@crypto_map_unlock_map_head.
CSCwf99947	Crash when modifying tunnel after running show crypto commands.
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.
CSCwh20577	Crashed by TRACK client thread at access invalid memory location.
CSCwh36801	Crash in IP Input process during tunnel encapsulation.
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.

Bug ID	Description
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

Open Bugs in Cisco IOS XE 17.12.2

Table 21: 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.
CSCwh99513	VPLS IRB not working when traffic came from VPNv4 and next-hop is learned over VPLS.
CSCwh91085	Convergence improvement after device reboot with mVPN profile 14.
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.
CSCwh99464	Guestshell connectivity not working with NAT overload.

Bug ID	Description
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.
CSCwh96332	Device crash due to dhcpd_binding_check.
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 .
CSCwf53750	"match pktlen-range" does not work with GRE/IPSEC GRE.
CSCwh60107	In the show tech file, "enable secret" does not get hidden.
CSCwh95024	ISIS crash in local uloop.
CSCwh41155	Wrong /32 self, complete map-cache entry for fabric hosts on iBN when overlapping summary exists.
CSCwi00680	Router unexpectedly reloads while using DHCP for ISG.
CSCwh96823	IOS-XE router not installing classless-static-routes from DHCP option 121.
CSCwh84850	Unexpected reboot in device due to SISF and STP initialization.
CSCwh21796	Password getting visible for the mask-secret in show logging.
CSCwf59929	CTS CORE process crash after configuring role based ACL.
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.
CSCwh99597	After migration MAC/IP only MAC is advertised.

Bug ID	Description
CSCwh75992	"BGP Router" process crash.
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.
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCwh10813	Add verbose log to indicate grant ra-auto un configures grant auto in PKI server.

Resolved Bugs in Cisco IOS XE 17.12.1a

Table 22: Resolved Bugs in Cisco IOS XE 17.12.1a

Bug ID	Description
CSCwd39257	IOS-XE cpp crash when entering **no ip nat create flow-entries**.
CSCwh67812	Unable to configure **crypto map** on a physical interface due to which crypto map-based VPN's cannot be formed.
CSCwf16332	HSRP loss communication with HSRP neighbor after two weeks of being configured.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwe66318	NAT entries expire on standby router.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwf48530	C1100TG incorrectly enters controller-managed mode.
CSCwf09370	Power supply unit showing empty in **show platform** output.
CSCwd76648	Port-channel DPI load-balancing not utilizing all the member-links.

Open Bugs in Cisco IOS XE 17.12.1a

Table 23: Open Bugs in Cisco IOS XE 17.12.1a

Bug ID	Description
CSCwf67564	RP3 observes memory leak at process SSS Manager.

Bug ID	Description
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.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwf49390	Device crashes@crypto_map_unlock_map_head.
CSCwf34171	Configure replace command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwh01095	Rapid memory leak on ngiolite process.
CSCwf99947	Crash when modifying tunnel after running **show crypto** commands.
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 interface, ack/seq number abnormal.

Resolved Bugs in Cisco IOS XE 17.9.6

Table 24: Resolved Bugs in Cisco IOS XE 17.9.6

Bug ID	Description
CSCwi08171	Router may crash due to Crypto IKMP Process.
CSCwi25737	Router should discard IKE Notification messages with incorrect DOI.
CSCwh50628	Race condition crash on IOS-XE device.
CSCwi68865	Memory leak in Crypto IKEv2 due to C_NewObject.
CSCwj88872	IPsec tunnel fails to establish due to error IPSec policy invalidated proposal.
CSCwi06404	PKI crash after failing a CRL Fetch.
CSCwi09301	Shutting a Dialer interface with PPPoA unshuts it automatically.
CSCwj84949	Unencrypted Traffic Due to Non-Functional IPsec Tunnel in FLEXVPN Hub & Spoke Setup.
CSCwj70335	Crypto IKEv2 - Fragmented Authentication packets detected as malformed on 3rd party vendor device
CSCwj08744	Unexpected reload when using "show running-config full | format" .
CSCwj92234	IR1833: UNIX-EXT-SIGNAL: Segmentation fault(11), Process = Cellular CNM.

Bug ID	Description
CSCwk12524	Device reloaded due to ezManage mobile app Service..
CSCwi93422	Unexpected reload due IPv6 TCP packet in QFP.
CSCwj45130	Segmentation Fault - Process = IPSec dummy packet process.
CSCwj48421	FlexVPN Client : IPsec tunnels are down due to issue with SADB detach and delete.
CSCwk15127	Failure to communicate a period of time after the stp status changes.
CSCwh96578	SKA_PUBKEY_DB leak in TDL.
CSCwj72888	Reload in tcp_sanity due to l4 pointer not set.
CSCwb47658	Repeated and endless messages "Network change event - activated 4G Carrier Aggregation."
CSCwf09370	Power supply unit showing empty in " show platform" output.

Open Bugs in Cisco IOS XE 17.9.6

Table 25: Open Bugs in Cisco IOS XE 17.9.6

Bug ID	Description
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error.
CSCwk27099	Cellular connection is picking the wrong profile.
CSCwm14665	Enable BFD L2 messages in the Punt path for platforms.
CSCwb55514	Unexpected reboot of the ESP seen after enabling "platform qos port-channel-aggregate".
CSCwh50510	Router Crash with Segmentation fault(11), Process = NHRP when processing NHRP traffic.
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwm27005	"CCA Detected Logic Error, code = 14" Traceback seen constantly.
CSCwj44868	GETVPN COOP KS | Wrong Severity for Rekey Acknowledgement configuration mismatch log message.
CSCwk63722	Startup Configuration Failure Post PKI Server Enablement.
CSCwk30527	IKEv2 session is down after reload if identity local address is assigned to interface on Switch.
CSCwk31560	NAT Command not readable after reloaded.
CSCwh45169	Unexpected Reboot while Dispalying Information from Cleared SSS Session.

Bug ID	Description
CSCwi16111	IPv6 tcp adjust-mss not working after delete and reconfigure.
CSCwk61133	Process IOMd memory leak due to POE TDL message.
CSCwi63042	Packet drops observe between LISP EID over GRE Tunnel.
CSCwm32269	Cisco DNA Center - SBEN Onboarding fails - EAP-TLS Failed to fetch IP address.
CSCwi62098	"show crypto ipsec sa output" command displays incorrect replay status.
CSCwh44418	ARP incomplete in VRF Mgmt-intf - G0/0/0 - Switch -G0.

Resolved Bugs in Cisco IOS XE 17.9.5

Table 26: Resolved Bugs in Cisco IOS XE 17.9.5

Bug ID	Description
CSCwh73350	Router keeps crashing when processing a firewall feature.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwf23291	Device: "write" or "do write" saves configuration but RSA keys /SSH lost after reload.
CSCwi28227	Router / IOS XE 17 / NAT HSL logging vrf-filter not working.
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCvo01546	NHRP reply processing may dequeue an unrelated request.
CSCwf03193	Device crash with crashinfo files were generated with Segmentation fault, Process IPSEC key engine
CSCwf16332	HSRP loss communication with HSRP neighbor after two weeks of being configured.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwh49644	CSDL Compliance failure : Use of 3DES by IPSec is denied.
CSCwf55243	Device is crashing while adding a trustpoint to the router .
CSCwh32386	Unexpected reload on router due to Critical process fman_fp_image in 17.9.3a.
CSCwf67564	Device observes Memory Leak at process "SSS Manager".
CSCwh30377	Device 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.
CSCwf96980	Unexpected reboot after configuring application redundancy.

Bug ID	Description
CSCwe64779	IOS XE router software forced reset during high IPC congestion with IPsec.
CSCwh20577	Crashed by TRACK Client thread at access invalid memory location.
CSCwh36801	Crash in IP Input process during tunnel encapsulation.
CSCwh96415	Can't disable DMVPN logging in IOS-XE 17.8 and higher.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwh20734	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is requested & deleted.
CSCwf71557	IPv4 connectivity over PPP not restored after reload.
CSCwc97579	Spoke-spoke cache refresh not working correctly in case of multiple cache entries for same next hop.
CSCwf04866	Keyman process crash seen while re-generating SSH key in device.
CSCwh00332	B2B NAT: when configration ip nat inside/outside on VASI intereface,ack/seq number abnormal.

Open Bugs in Cisco IOS XE 17.9.5

Table 27: Open Bugs in Cisco IOS XE 17.9.5

Bug ID	Description
CSCwi08171	Router may crash due to Crypto IKMP Process.
CSCwe24491	Device: Static NAT with HSRP stops working after removing / adding standby.
CSCwi53951	Packets with Unicast MAC get dropped on a Port Channel L2 Sub-intf after a router reboot.
CSCwh80441	Cosmetic 3G issue causing distress to customers - Modem WCDMA 900 is displayed as Unknown.
CSCwh18120	IKEv2 - diagnose feature is taking 11% CPU during session bring up.
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error.
CSCwi06404	PKI crash after failing a CRL Fetch.
CSCwh50510	Router Crash with Segmentation fault(11), Process = NHRP when processing NHRP traffic.
CSCwi25737	Router should discard IKE Notification messages with incorrect DOI.
CSCwi46997	NAT Command not readable after reload.
CSCwi51326	CPP CP SVR crash after decoding all packets to text (using l2 copy) on fia trace.

Bug ID	Description
CSCwi63042	Packet drops observe between LISP EID over GRE Tunnel.
CSCwc30418	Segmentation fault observed in ikev2_dupe_delete_reason.
CSCwi16111	IPv6 tcp adjust-mss not working after delete and reconfigure.
CSCwi10735	ZBF drops transit WAAS PSH/ACK packet due to 'Invalid ACK number'.
CSCwh91136	IOS XE: Traffic not encrypted and droped over IPSEC SVTI tunnel.

Resolved Bugs - Cisco IOS XE 17.9.4a

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 17.9.4a

There are no open bugs in this release.

Resolved Bugs in Cisco IOS XE 17.6.8a

There are no resolved bugs for this release.

Open Bugs in Cisco IOS XE 17.6.8a

There are no open bugs in this release.

Resolved Bugs in Cisco IOS XE 17.6.7

Table 28: Resolved Bugs in Cisco IOS XE 17.6.7

Identifier	Headline
CSCwh73350	Router keeps crashing when processing a firewall feature.
CSCvo01546	NHRP reply processing may dequeue an unrelated request.
CSCwh49644	CSDL Compliance failure : Use of 3DES by IPSec is denied.
CSCwh20577	Crashed by TRACK Client thread at access invalid memory location.
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 in Cisco IOS XE 17.6.7

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 in Cisco IOS XE 17.6.6a

Table 29: Open Bugs in Cisco IOS XE 17.6.6a

Bug ID	Description
CSCwh01095	Rapid memory leak on ngiolite process.

Resolved Bugs in Cisco IOS XE 17.6.6

Table 30: Resolved Bugs in Cisco IOS XE 17.6.6

Bug ID	Description
CSCwf47563	Device is crashing after importing the trustpoint with rsakeypair.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit.
CSCwf09370	Power supply unit showing empty in **show platform** output.
CSCwf16332	HSRP loss communication with HSRP neighbor after two weeks of being configured.

Open Bugs in Cisco IOS XE 17.6.6

Table 31: Open Bugs in Cisco IOS XE 17.6.6

Bug ID	Description
CSCwh01095	Rapid memory leak on ngiolite process.

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 in Cisco IOS XE 17.6.5a

No open bugs in this release.

Resolved Caveats - Cisco IOS XE 17.3.8a

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 in Cisco IOS XE 17.3.8a

No open bugs in this release.

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.