Release Notes for Cisco 1000 Series Integrated Services Routers, Cisco IOS XE Cupertino 17.9.x

First Published: 2022-08-26

Last Modified: 2024-02-28

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 Cupertino 17.9.1a is the first release for Cisco 1000 Series Integrated Services Routers in the Cisco IOS XE Cupertino 17.9.x release series.

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

Table 1: New Software Features

Feature	Description
Support for Unicast-to-Multicast Destination Reflection	This feature introduces support for configuration of unicast-to-multicast destination reflection to facilitate unicast-to-multicast destination translation and unicast-to-multicast destination splitting. It also provides the capability for users to translate externally received unicast destination addresses to multicast addresses.
Support for BGP additional paths with label-unicast unique mode	This enhancement introduces support for configuring BGP additional paths when label-unicast unique mode is configured
Cube Features	

Feature	Description
CUBE: End-to-end Secure Calling for Courtesy Call Back and Unified Contact Center Survivability	With the Cisco Voice Portal (CVP) application, a caller may request an automatedcallback, rather than wait in a queue for an extended period. When an agent becomes available, CVP sends a request to place a call to the original caller. When the call is answered, the agent is connected. With this update, outbound calls over a secure SIP PSTN trunk are possible.
CUBE: Options Ping for DNS SRV Hosts	Previously, CUBE (Local Gateway) had to be configured with separate dial-peers to monitor the availability of individual proxies used in services such as Webex Calling. To simplify this configuration, all targets resolved from a DNS SRV record may now be monitored using a common Options Ping policy defined for a single dial-peer. If a remote server becomes unresponsive, CUBE will busy out that destination, allowing calls to be sent to alternative destinations.
Transfer of Call Detail Records Using SFTP	Cisco IOS gateways can use FTP and now SFTP servers to transfer call accounting files.
Webex Calling Branch Survivability	From Unified SRST 14.3, new CLI commands are introduced to support the forthcoming Webex Calling Site Survivability mode. This feature will only be available for use when the Webex Calling Site Survivability solution is made available through Webex Control Hub.
Programmability Features	
Pubd Restartability	The pubd process is restartable on all platforms in this release. Prior to this release, pubd was restartable only on certain platforms. On other platforms, to restart the pubd process, the whole device had to be restarted.
Smart Licensing Using Policy Features	
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).
Inconsistent system behavior for **license boot** global configuration command rectified.	The system does not allow overlapping suite and technology package configuration to co-exist. For more information, see license boot.

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).
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. **Note** When using a VRF, the supported transport types are **smart** and **cslu** only.) For more information, see license smart (global config)

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.

Note From the Cisco IOS XE 17.9.2a release, the 5G sub-6 GHz Pluggable Interface Module (PIM) P-5GS6-GL is supported on the Cisco 1000 Series Integrated Services Routers.

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 17.9.4

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.3a

There are no new software features in this release.

New and Changed Software Features in Cisco IOS XE 17.9.2a

There are no new software features in this release.

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 and recommended ROMmon version is 17.6(1r).
- If the manufacturing date is less than 0x2535, the ROMMON will be automatically upgraded to 17.5(1r) 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.

Table 2: 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)

Cisco IOS XE Release	Minimum ROMmon Release for IOS XE	Recommended ROMmon Release for IOS XE
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)
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)

Resolved and Open Bugs in Cisco 1000 Series Integrated Services Routers

Resolved Bugs in Cisco IOS XE 17.9.5a

Bug ID	Description
CSCwf16332	HSRP loss communication with HSRP neighbor after two weeks of being configured.
CSCwf41450	Device reloads changing the resource profile.
CSCwi40697	Modem may not come back up from FW upgrade with LM960A18 and FN980 modems.
CSCwf61720	Device "No licenses in use" after upgrading from traditional to Smart Licensing IOS-XE versions.
CSCwh73350	Router keeps crashing when processing a firewall feature.
CSCwf67564	Device observes memory leak at process "SSS Manager".
CSCwf23291	Device "write" or "do write" saves configuration but RSA keys /SSH lost after reload.
CSCwc79115	cEdge Policy commit failure notification and alarm from vSmart.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.

Bug ID	Description
CSCwh68508	Unexpected reboot after establishing control plane of EVPN MPLS and receiving packets.
CSCvo01546	NHRP reply processing may dequeue an unrelated request.
CSCwf82676	CPU usage mismatch in "sh sdwan system status" vs "sh proc cpu platform"
CSCwf03193	Device crash with crash info files were generated with Segmentation fault, Process IPSEC key engine.
CSCwh08434	OMP route is being advertised although the route is not available.
CSCwf26875	Ten0/0/2 from Port-channel going to suspended status applying "platform qos port-channel-aggregate"
CSCwf24164	Netflow stops working when flow monitor reaches cache limit in device.
CSCwh63061	Telstra Cert: FN980 modem (P-5GS6-GL) is showing 4 additional NR bands support - 1, 3, 7, and 28
CSCwi28227	IOS XE 17 - NAT HSL logging vrf-filter not working.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwe91898	Environmental syslog is not appearing when power cord is disconnected from the redundant PS.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwh49644	CSDL Compliance failure : Use of 3DES by IPSec is denied.
CSCwh32386	Unexpected reload on device due to Critical process fman_fp_image in 17.9.3a
CSCwe30514	Device reboots with sslproxy and utd enabled
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.
CSCwe64779	IOS XE router software forced reset during high IPC congestion with IPsec.
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 device.
CSCwh36801	Crash in IP Input process during tunnel encapsulation.
CSCwh96415	Can't disable DMVPN logging in IOS-XE 17.8 and higher.

Bug ID	Description
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.
CSCwf11394	IOS XE - Vdaemon debug log should mention port-hop and reason prior to DISTLOC.
CSCwf04866	Keyman process crash seen while re-generating SSH key in device.
CSCwh00332	B2B NAT: when configuration IP NAT inside/outside on VASI interface,ack/seq number abnormal.

Open Bugs in Cisco IOS XE 17.9.5a

Bug ID	Description
CSCwi10735	ZBF drops transit WAAS PSH/ACK packet due to 'Invalid ACK number'.
CSCwi07148	Interfaces configuration change from negotiation auto to no negotiation auto after a reboot.
CSCwi60071	IPv6 PREFIX delegation is not working on ADSL PPPOA.
CSCwi51326	CPP CP svr crash after decoding all packets to text (using l2 copy) on fia trace.
CSCwh01678	Router FTM crash with SIG enabled.
CSCwh80441	Cosmetic 3G issue causing distress to customers - Modem WCDMA 900 is displayed as unknown.
CSCwi06843	Endpoint tracker triggers a CPU Hog.
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.
CSCwh50510	Router Crash with Segmentation fault(11), Process = NHRP when processing NHRP traffic.
CSCwi33168	DSP reporting out of range utilization values in SNMP.
CSCwi08171	Router may crash due to Crypto IKMP Process.
CSCwh12093	Enable SoS/ROC feature for DSL.
CSCwf84960	Device LED L remains green after port shutdown.
CSCwh18120	IKEv2 - diagnose feature is taking 11% CPU during session bring up.

Bug ID	Description
CSCwh41497	DDNS update retransmission timer fails to work with a traceback error.
CSCwi04547	Device Custom Application is marked as invalid.
CSCwi25737	Router should discard IKE Notification messages with incorrect DOI.
CSCwi06404	PKI crash after failing a CRL Fetch.
CSCwh22414	Warning and critical CPU utilization thresholds not recomputed when using data-plane-heavy mode.
CSCwi46997	NAT Command not readable after reloaded.
CSCwi01046	PoE module is not providing enough power to bring the ports after an unexpected reload.
CSCwc30418	Segmentation fault observed in ikev2_dupe_delete_reason.
CSCwi16111	IPv6 tcp adjust-mss not working after delete and reconfigure.
CSCwi63042	Packet drops observe between LISP EID over GRE Tunnel.
CSCwi53306	Unknown app ID in ZBFW HSL log.
CSCwb25507	CWMP : Add vendor specific parameter for NBAR protocol pack version.
CSCwi59202	MFG Manhattan can't boot up in IOS.
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 in Cisco IOS XE 17.9.4a

Bug ID	Description
CSCwd39257	IOS-XE cpp crash when entering **no ip nat create flow-entries**.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwf41492	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
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.

Bug ID	Description
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites.
CSCwf34171	Configure replace command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.
CSCwf41450	Device reloads changing the resource profile.
CSCwf52751	CLI template fails to attach to device with error access-denied.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list.
CSCwf03193	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine.
CSCwf11394	IOS XE - debug log should mention port-hop and reason prior to DISTLOC.
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config.
CSCwf61720	No licenses in use after upgrading from traditional to smart licensing IOS-XE versions.
CSCwe51910	SNMP if index persist does not work.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit.
CSCwd61988	Output packet bytes calculation biased when we enable QoS on port channel.
CSCwf25735	QoS more than four remark with set-cos not work.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.

Resolved Bugs in Cisco IOS XE 17.9.4

Bug ID	Description
CSCwf48808	FlexVPN: Stale client routes stuck in RIB on FlexServer.
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
CSCwf02225	Device freezes on using show sdwan commands.
CSCwe24210	SNMP MIB does not show correct firmware version for LTE module.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwf08698	Device crashes unexpectedly due to a fault in the 'TLSCLIENT_PROCESS'.

Bug ID	Description
CSCwf47796	NHRP cache entries flood matching a /32 default route.
CSCwf09758	Crashes while importing big CRL file into switch.
CSCwe12194	Auto-update cycle incorrectly deletes certificates.
CSCwd49309	uCode crash seen on thorium with traffic pointing to segfault in coff handler.
CSCwe33793	Memory allocation failure with extended antireplay enabled.
CSCwe66318	NAT entries expire on standby router.
CSCwa96399	Configuring entity-information xpath filter causes syslogs to print, does not return data.
CSCwe20008	SNMP MIB OID changing its last index.
CSCwf47563	Device is crashing after importing the trustpoint with rsakeypair.
CSCwe18058	Unexpected reload with IPS configured.
CSCwd73783	Observed qfp-ucode-wlc crash.
CSCwe39011	GARP on port up/up status from router is not received by remote peer device.
CSCwe83169	Pseudowire control word not working on device.
CSCwf39490	MCID (Malicious Call Identification) gets broken due to custom prefix setting under STCAPP FAC.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwe69783	Device can lose its config during a triggered resync process if lines are in an off-hook state.
CSCwe89404	No way audio when using secure hardware conference with secure endpoints.
CSCwe41234	VMWI race condition causes no ringing for analog phones.
CSCwc89823	Router crashes due to CPUHOG when walking ciscoFlashMIB @snmp_platform_get_flash_file_info.
CSCwe32862	Router IOS-XE crash while executing AES crypto functions.
CSCwf37888	Packet duplication: Duplicate packets are counted on primary tunnel interface statistics.
CSCwd68994	ISAKMP profile does not match as per configured certificate maps.
CSCwd35047	Failed to ping gateway while configuring shared LOM with console, te1 interface until router reload.
CSCwd49177	ISG: L2-connected subscriber: IPv6 prefix delegation is not reachable when packets are switched.

Bug ID	Description
CSCwe70374	Device punt-policer is not configurable.
CSCwe37123	Device uses excessive memory when configuring ACLs with large object groups.
CSCwd59722	Unexpected reboot due to IOSXE-WATCHDOG: Process = Crypto IKMP.
CSCwe31471	Segmentation fault in SDWAN PB rx when per-tunnel QoS config withdraw.
CSCwd87195	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.
CSCwe18124	MACSEC remains marked as SECURED, but randomly the traffic stops working.

Open Bugs in Cisco IOS XE 17.9.4

Bug ID	Description
CSCwd39257	IOS-XE cpp crash when entering **no ip nat create flow-entries**.
CSCwe85301	Crypto PKI-CRL-IO_0 process crash when PKI trustpoint is being deleted.
CSCwf41492	NHRP BFD flaps randomly with dynamic tunnel (NHRP phase 3) in DMVPN.
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.
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites.
CSCwf34171	Configure replace command fails due to the license udi PID XXX SN:XXXX line on IOS-XE devices.
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.
CSCwf41450	Device reloads changing the resource profile.
CSCwf52751	CLI template fails to attach to device with error access-denied.
CSCvz82148	%CRYPTO_SL_TP_LEVELS-6-VAR_NEW_VALUE message is observed in each write config with same crypto value.
CSCwf55243	Device is crashing while adding a trustpoint to the router.
CSCwe95072	Unexpected reload due to memory corruption when modifying and access list.
CSCwf03193	Device crash with crashinfo files were generated with segmentation fault, process IPSEC key engine.
CSCwf11394	IOS XE - debug log should mention port-hop and reason prior to DISTLOC.
CSCwf00276	Packets with L2TP headers cause device to crash.
CSCwf60120	Static NAT entry gets deleted from running config; but remains in startup config.

Bug ID	Description
CSCwf61720	No licenses in use after upgrading from traditional to smart licensing IOS-XE versions.
CSCwe51910	SNMP if index persist does not work.
CSCwf24164	Netflow stops working when flow monitor reaches cache limit.
CSCwd61988	Output packet bytes calculation biased when we enable QoS on port channel.
CSCwf25735	QoS more than four remark with set-cos not work.
CSCwf51206	EVPN: BUM traffic is not flooded to bridge domain interface.
CSCwh60848	CUBE - SIP Message Queuing Fails to Resume Transmission

Resolved Bugs in Cisco IOS XE 17.9.3a

Bug ID	Description
CSCwd45402	MSR Unicast-To-Multicast not working if destination and source are the same in service reflect configuration.
CSCwd90168	Unexpected reload after running **show voice dsp** command while an ISDN call disconnects.
CSCwd16559	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table.
CSCwd79089	Device controller crash when sending full line rate of traffic with >5 Intel AX210 stations.
CSCwc27307	Service Engine YANG support for ZBFW.
CSCwd16664	GetVPN long SA - GM re-registration after encrypting 2^32-1 of packets in one IPSEC SA.
CSCwd81357	QoS classification not working for DSCP or ACL + MPLS EXP.
CSCwd89338	Clear ISG existing lite-session upon reception of DHCP packet for same client.
CSCwc99823	FMAN crash seen in SGACL@ fman_sgacl_calloc.
CSCwd25107	Interface VLAN1 placed in shutdown state when configured with ip address pool.
CSCwd61255	Data plane crash on device when making per-tunnel QoS configuration changes with scale.
CSCwe01015	IKEv2/IPSec - phase 2 rekey failing when peer is behind NAT.
CSCwd85580	Device unexpected reload after set **ospfv3 authentication null** command.
CSCwd03869	CEF DPI load-balancing causes out of order packets.
CSCwc65697	Device crashing and restarting during call flow with new image.

Bug ID	Description
CSCwd84599	Dataplane memory utilization issue - 97% QFP DRAM memory utilization.
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through router.
CSCwd15487	[MBPL Integration] Kernel crash is observed when modem-power-cycle is executed.
CSCwd38943	GETVPN: KS reject registration from a public IP.
CSCwd06372	Unconditional excessive logging in eogre tunnel error handling case.
CSCwe03614	CWMP : MAC address of ATM interface is not included in inform message.
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number (<1M).
CSCwd33202	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface.
CSCwd06923	Stale ip alias left after NAT statement got removed.
CSCwd47123	ISG uses identifier mac-address 0000.0000.0000 when DHCP LQ does not reply.
CSCwd72312	GETVPN : Traffic drops seen on GM after rekey installing policies.
CSCwc14688	Single WAN interface subslot 0/0 timing.
CSCwd07516	Memory leak under linux_iosd-image related to SNMP.

Open Bugs in Cisco IOS XE 17.9.3a

Bug ID	Description
CSCwd39257	IOS-XE cpp crash when entering **no ip nat create flow-entries**.
CSCwd63783	Memory leak caused router reload.
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected.
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwe14885	VPN is established although the peer is using a revoked certificate for authentication.
CSCwe24491	Static NAT with HSRP stops working after removing/adding standby.
CSCwe32827	NIM-LTEA-EA module incorrectly shows "Profile 1 = INACTIVE*".
CSCwd17272	UTD packet drop due to fragmentation for ER-SPAN traffic.
CSCwe32862	Router IOS-XE crash while executing AES crypto functions.
CSCwc28468	Device always fails to push any template to device if device is running in FIPS mode.
CSCwd68994	Unable to match on customer profile based on certificate-map.

Bug ID	Description
CSCwc06327	PFP policy in SRTE, RIB resolution in FC bring down ipsec tunnel interface- stuck at linestate down.
CSCwe38732	IP CEF load sharing command is being changed by the device.
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwh60848	CUBE - SIP Message Queuing Fails to Resume Transmission

Resolved Bugs in Cisco IOS XE 17.9.2a

Bug ID	Description
CSCwc21739	NAT not requesting further for low ports after initial allocation when CLI knob reserved-ports set.
CSCwc39012	Crash saving tracelogs after "Too many open files" error.
CSCwc03478	vTCP does not support L2 correctly.
CSCwc72923	ERROR info: Router configuration failed:interface Serial0/1/0:23 isdn switch-type primary-ntt.
CSCwd12591	UCode crash during FW classification, session frees.
CSCwc99668	Routes added by IKEv2 getting deleted at responder.
CSCwc23077	Firewall drop seen stating “FirewallL4” seen on device.
CSCwc44851	Bootstrap failing on device.
CSCwc96444	Device is not programming correct next-hop for unicast prefix with multicast config present.
CSCwc49715	Crash @ UNIX-EXT-SIGNAL: Aborted(6), Process = Check heaps, having PPPoe with cwmp configs.
CSCwd06118	IKEv2 cert-based IPsec not working between IOS-XE and AWS.
CSCwb52324	Device unexpected reload due to QFP UCode crash.
CSCwc77183	Packet duplication is causing drops in payment transactions.
CSCwc20170	Device reloads unexpectedly due to critical FTMD fault when VRF configuration is pushed
CSCwb89958	Unified policy HSL not sending proper NBAR application information.
CSCwc89328	Multiple devices experience crashes every 4-5 minutes.
CSCwc52538	Device flows are not distributed and load-balanced evenly and consistently.
CSCwc45950	ZBFW self zone policy drops SSH session on mgmt-intf 512 ports.

Bug ID	Description
CSCwc43794	Device VRF+NAT outside source static - drop packets during FTP (active-mode) execution.
CSCwc79145	Throughput degrades when local TLOC specified in data policy goes down.
CSCwc37603	Slot 0/1 crash after changing switchport with allowed wide range VLANs from trunk to access.
CSCwc32595	BFD sessions remains down if interface flap form up/down/up.
CSCwb65396	CLI template push fails with error: 'Error: on line 48: line-mode single-wire line 0'.
CSCwb90252	Automatically freeing up filesystems stale image or recovered folder (lost+found).
CSCwc82140	QFP crash when ZBFW configuration features "log dropped-packets" configuration.
CSCvz89354	Router running crashes due to CPUHOG when walking ciscoFlashMIB.
CSCwc39865	Subscriber session getting stuck and needs clearing it manually.
CSCwb48953	Device speed test failing with "Device error: Speed test in progress".
CSCwd11365	Needs cert update - Azure CGW creation fails due to NVA provisioning failure.
CSCwc54463	LAN module is down when high CPU noticed.
CSCwb08057	ISG: Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
CSCwc29629	Crashes when virtual-access tries to bring-up/bring-down OSPFv3 IPsec crypto session authentication.
CSCwc36910	Device pushes wrong (typo) syntax as "config wlan broadcase-ssid disable 2".
CSCwd13352	SSH from vshell to device getting closed after update.
CSCwc77177	BFD and control packets are dropped when ACL is applied on gigi to which loopback is bind.
CSCwc68132	SIG tunnel tracker packets are dropped by firewall with self zone policy.
CSCwd56336	BFD sessions are not coming up after flapping the interface due to low ftm rate.
CSCwd56015	UTD skipped when interface UTD config is used to enable/disable UTD.

Open Bugs in Cisco IOS XE 17.9.2a

Bug ID	Description
CSCwd45508	Device does not form BFD across serial link when upgrading.
CSCwd23810	A high CPU utilization caused by NHRP.

Bug ID	Description
CSCwd38626	Repeating SYS-2-PAK_SUBBLOCK_BADSIZE: 4 -Process= <interrupt level>.
CSCwd13050	After upgrade, device moved into Out of Sync status.
CSCwd12955	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured.
CSCwc28468	Device always fails to push any template if it is running in the FIPS mode.
CSCwd36621	CERM may kick in due to IPsec sessions initiated for on-demand tunnels.
CSCwc99823	fman crash seen in SGACL@ fman_sgacl_calloc.
CSCwd17579	Nutella router crashing with reason CPU usage due to memory pressure exceeds threshold (reboot).
CSCwd34941	NAT configuration with no-alias option is not preserved after reload.
CSCwd33966	Unable to configure the local BGP as-path-list.
CSCwd37410	0365 and MS Teams applications access issues when using DIA with app-list match in data-policy.
CSCwd15560	With 2 sequences, should not skip if the match is different and action is same.
CSCwc37465	Unable to push no-alias option on static NAT mapping from management system.
CSCwa92817	SNMP polling not working on PPP Interface.
CSCwd44006	Control connection on device does not come up with reverse proxy using enterprise certificate.
CSCwd29334	Upgrade failures due to inability to establish NETCONF connection from device to upgrade-confirm.
CSCwc88791	DSL: Erroneous atm interface counter at DSL retraining.
CSCwa96399	Configuring entity-information xpath filter causes syslogs to print, does not return data.
CSCwd44586	Login banner config is changed after upgrade.
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through router.
CSCwc76082	check_sig_ipsec_ike_sessions fails with could not find entry for Tunnel100001.
CSCwa14636	Device stopped forwarding traffic. Suspect OMPD is busy.
CSCwc38529	Traffic seems not inspected by UTD when umbrella is set.
CSCvz55282	Serviceability enhancements for config migration failures between releases.
CSCwd33202	DHCP behavior issue when BDI interface is enabled on WAN and SVI interface.

Bug ID	Description
CSCwd17381	NAT/DIA traffic is skipping UTD in forward direction after SSNAT path from service-side.
CSCwc70511	Router reloads unexpectedly during NHRP processing.
CSCwd18028	After delete CSP, new CCM bring up on existing CSP is stuck in "Initializing CCM" on MT cluster.

Resolved Bugs in Cisco IOS XE 17.9.1a

Table 3: Resolved Bugs in Cisco IOS XE 17.9.1a

Bug ID	Description
CSCvz65764	Peer MSS value showing incorrect.
CSCwa95092	When object-group used in a ACL is updated, it takes no effect.
CSCwb33968	Device failed to display active flows when flow count is high on the device.
CSCwb02142	Traceback: fman_fp_image core after clearing packet-trace conditions
CSCwb49857	Memory leaks on keyman process when key is not found.
CSCwb59736	CSR BFD tunnel are zero.
CSCwa65728	Large number of DH failures.
CSCwb11389	NAT translation stops suddenly (ip nat inside does not work).
CSCwa84919	Revocation-check crl none does not failover to NONE DNAC-CA.
CSCwb39098	Router crashed after new IPv6 address assigned when router use specific configuration.
CSCwa69101	ISG: initiator unclassified ip-address LQipv4 command has no effect.
CSCwa67886	UDP based DNS resolution does not work with IS-IS EMCP on IOX-XE.
CSCvz84588	Destination prefix packets getting dropped because forwarding plane is not programming the next hop.
CSCwb27486	New key for NBAR app and NBAR category without OGREF optimized.
CSCwa49101	OMP origin protocol comparison cleanup.
CSCwb17282	Router crashing when clearing a VPDN session.
CSCwa49721	HUB with firewall configured incorrectly dropping return packets when routing between VRFs.
CSCwb38501	Device support IGMP on voice vlan.
CSCwa51582	IP device-tracking not functional with voice VLAN configured.

Bug ID	Description
CSCwb12647	Device crash for stuck threads in cpp on packet processing.
CSCwb18223	SNMP v2 community name encryption problem
CSCwb16723	Traceroute not working on device with NAT.
CSCwb31587	Subject-alt-name attribute in certificate trustpoint causes Windows NDES/CA to reject SCEP requests.
CSCwb51238	Router reload unexpectedly two times when enter netflow show command.
CSCwa98617	Memory leak in AEM chunks related to firewall.
CSCwa48512	CoR intercepted DNS reply packets dropped with drop code 52 (FirewallL4Insp) if UTD enabled also.
CSCwa93664	ThousandEyes container may fail to get installed on device.
CSCvz28950	DMVPN phase 2 connectivity issue between two spokes.
CSCwa78348	Traceback: IOS-XE reload after segmentation fault on process = SSS manager.
CSCvz81664	Enabling or disabling OMP overlay as prevents connected routes from being advertised in OMP.
CSCwa67029	ROMmon version not displaying correctly.
CSCwb43423	IOS XE image installation fails.
CSCwa08847	ZBFW policy stops working after modifying the zone pair.
CSCwb15331	Keyman memory leak using public keys.
CSCvw50622	NHRP network resolution not working with link-local IPv6 address.
CSCwb21645	NAT traffic gets dropped when default route changes from OMP to NAT DIA route.
CSCwa57873	Incorrect reload reason - Last reload reason: LocalSoft for Netconf initiated request.
CSCwb51595	Missing IOS config (voice translation rule) on upgrade.
CSCwb18315	Umbrella DNS security policy does not work with cloud on ramp with SIG tunnels.

Open Bugs in Cisco IOS XE 17.9.1a

Table 4: Open Bugs in Cisco IOS XE 17.9.1a

Bug ID	Description
CSCwc39012	Crash saving tracelogs after too many open files error.
CSCwc56896	Crash in ipv6_tunnel_macaddr while adding/removing gre multi-point tunnel mode.

Bug ID	Description
CSCwb89958	Unified policy HSL not sending NBAR application information properly.
CSCwc23077	Firewall drop seen stating “FirewallL4” seen on device.
CSCwb74821	Yang-management process confd is not running.
CSCwc44851	Bootstrap failing on device.
CSCwc55684	Device SIG GRE: Layer 7 health check does not work on loopback interfaces.
CSCwc49715	Crash at UNIX-EXT-SIGNAL: aborted(6), process = check heaps, having PPPoE with CWMP configs.
CSCwc52538	Device flows are not distributed and load-balancing is even and consistent.
CSCwc55260	Device memory leak due to FTMd process.
CSCwc69881	Device lost configuration due to multiple power cycles on site.
CSCwc20170	Device reloads unexpectedly due to critical FTMD fault when VRF configuration is pushed.
CSCwb88621	Device unable to establish control connection with vBond due to out of order DTLS packets.
CSCwc37465	Static NAT configuration in CLI with the no-alias keyword cannot be retrieved via NETCONF/YANG.
CSCwc59598	Device statistics collection causing service-side BFD to flap on every collection interval.
CSCwc50477	Device crashed in ipv4_nat_create_out2in_session_entry.
CSCwc67465	Router can not be upgraded.
CSCwc32595	BFD sessions remains down if interface flap form up/down/up.
CSCwc38529	Traffic seems not inspected by UTD when umbrella is set.
CSCwc63563	Unable to set specific speed and duplex values on SFP ports on IOS-XE routing platforms.
CSCwc39865	Subscriber session getting stuck and needs clearing it manually.
CSCwc43973	DLC is not completing after upgrading to Smart Licensing from CSL.
CSCwc53885	IOS-XE "no ip nat" config is allowed to be committed and removes nat routes among other nat config.
CSCwc55467	BFD tunnel on router is not staying up, 1 out of 40 tunnels.
CSCwc54463	LAN Module is down when high CPU noticed.
CSCwc42978	Device looses all BFD sessions with invalid SPI.

Bug ID	Description
CSCwc67171	Tracebacks at cgm_avlmgr_class_init and cpuhog_key_init.
CSCwb08057	Number of lite sessions conversion in progress counter not decrementing on failed account-logon.
CSCwc63337	Destination not reachable if configured as a next for a static route resolvable via non /32 OMP.
CSCwc29629	Crashes when virtual-access tries to bring-up/bring-down OSPFv3 IPsec crypto session authentication.
CSCwc27208	BFD sessions not coming up because of ANTI-REPLAY-FAILURES.
CSCwc68132	SIG tunnel tracker packets are dropped by firewall with self zone policy.
CSCwc14688	Single WAN interface subslot 0/0 timing.
CSCwc70511	Router reloaded unexpectedly.

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 Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

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

Documentation Feedback

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

Troubleshooting

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

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