Release Notes for Cisco Catalyst 8500 SeriesEdge Platforms, Cisco IOS XE Bengaluru 17.5

First Published: 2020-04-14

About Cisco Catalyst 8500 Series Edge Platforms

Note Cisco IOS XE Cupertino 17.9.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE Cupertino 17.9.x release series.

The Cisco Catalyst 8500 Series Edge Platforms are high-performance cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

The Cisco Catalyst 8500 Series Edge Platforms includes the following models:

- C8500-12X4QC
- C8500-12X
- C8500L-8S4X

For more information on the features and specifications of Cisco 8500 Series Catalyst Edge Platform, refer the Cisco 8500 Series Catalyst Edge Platform datasheet.

Sections in this documentation apply to all models of unless a reference to a specific model is made explicitly.

New and Changed Software Features

Note Starting from IOS XE 17.5, the following platforms will move to monolith packaging and therefore it will not be possible to upgrade/downgrade using separate packages:

- C8500-12X4QC
- C8500-12X
- C8500L-8S4X

Instead use the command **install add file bootflash:<file name> activate commit** command to upgrade using a single image that combines all the separate packages therefore improving the boot time.

Note Starting from IOS XE 17.6, the ISSU on Cisco Catalyst 8500 Edge Platforms will migrate to an install workflow that provides step-by-step upgrade/downgrade commands.

The ISSU load version commands will be deprecated and these commands include:

- abortversion
- acceptversion
- checkversion
- commitversion
- config-sync
- image-version
- loadversion
- runversion

Additionally, dual IOSd ISSU commands and Bundle mode ISSU workflows will also be disabled.

Table 1: Software Features

Feature	Description
Traffic Steering by Dropping Invalid Paths	If the SR-TE Policy has no valid paths defined, the paths are dropped and traffic being steered through the policy falls back to the default (unconstrained IGP) forwarding path. Also, when a SR-TE policy carrying best-effort traffic fails, traffic is re-routed and this impacts the SLA for premium traffic.To solve this issue, if the SR-TE policy fails, the traffic in the data plane is dropped but kept in the control plane. Therefore, other SR policies, potentially carrying premium traffic, are not impacted.
Enabling Segment Routing Flexible Algorithm with IS-IS	• Segment Routing Flexible Algorithm allows operators to customize IGP shortest path computation according to their own needs. An operator can assign custom SR prefix-SIDs to realize forwarding beyond link-cost-based SPF. As a result, Flexible Algorithm provides a traffic engineered path automatically computed by the IGP to any destination reachable by the IGP • Flex Algo prefix metric: Flex-algo prefix-metric allows to associate metric computed in given flex-algo with a prefix during prefix inter-level leaking or during inter-domain redistribution .This help to compute optimal inter-level or inter-domain path • Support for affinities include any/all: Ability to pick and choose the links that they want. User can use a certain path without creating a label stack by using the Prefix SIDs or Adjacency SIDs • TI LFA and uLoop Avoidance : Allows computation of Loop Free Alternate (LFA) paths. TI-LFA backup paths using the same constraints as the calculation of the primary paths for Flexible Algorithms, for IS-IS Inter-area leaking of Flexible Algorithm SIDs and prefixes and selectively filtering the paths that are installed to the MFI are also supported .

Feature	Description
View traffic counters for SR-TE policies	The existing command **show segment-routing traffic-eng policy** is improved to display the traffic rate on the tunnel interface. No configuration is required to enable this feature.
IS-IS Local Unequal Cost Multipath	This feature allows you to configure load balancing of outgoing traffic across all IGP ECMP paths proportionally to the interface bandwidth.
Configuring a limit on mroutes	This feature lets you configure a limit to the number of mroutes on an interface. By limiting the mroutes, you can avoid the risk of flooding the network with mroutes therefore protecting the router from resource overload and also preventing DoS attacks.
Tunnel Path MTU Discovery on MPLS-enabled GRE Tunnel	You can now use the **tunnel mpls-ip-only** command to configure how the Do Not Fragment bit from the payload is copied into the tunnel packets IP header.If the Do Not Fragment bit is not set, the payload is fragmented if an IP packet exceeds the MTU set for the interface.
License Management for Smart Licensing Using Policy, Using Cisco vManage	Cisco SD-WAN operates together with Cisco SSM to provide license management through Cisco vManage for devices operating with Cisco SD-WAN. For this you have to implement a topology where Cisco vManage is connected to CSSM. For information about this topology, see the Connected to CSSM Through a Controller, and to know how to implement it, see the Workflow for Topology: Connected to CSSM Through a Controller sections of the *Smart Licensing Using Policy for Cisco Enterprise Routing Platforms*guide. For more information about Cisco vManage, see the License Management for Smart Licensing Using Policy section of the *Cisco SD-WAN Getting Start Guide*. For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the features, platform, and software image support on Cisco Catalyst 8500 Series Edge Platforms. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/ An account on cisco.com is not required.

Resolved and Open Bugs for Cisco IOS XE Bengaluru 17.5

Resolved Bugs for Cisco IOS XE Bengaluru 17.5

Caveat ID Number	Description
CSCvp65521	vManage rel 18.3.5 - Service Side WAN Edge VPN - can't use Optional AdvertiseOMP>Aggregate field
CSCvt58920	SIM failover within the same modem takes long time to detect LTE network for AT&T
CSCvu97660	dataplan crash seen at pppoe

Caveat ID Number	Description
CSCvv19063	ASR 1000, C9800 Commit config clean up for cstate and pstate to 17.4, 17.3.2, 17.2.2: backout idle=poll
CSCvv25049	Number of EoGRE sessions count are not matching on fugazi
CSCvv28030	Greenday: IQDFZ profile degraded by 8% after BLD_POLARIS_DEV_LATEST_20200801_051231
CSCvv33576	IGMP snooping table not populated on ISR4k
CSCvv34691	NAT session scale causes tracebacks @%HW_FLOWDB-3-HW_FLOWDB_DBLINSTALL_FEATOBJ
CSCvv37172	License lost after "no license boot level <>" CLI followed by reset button
CSCvv38438	Watchdog timeout due to Crypto IKMP
CSCvv44331	AppQoe Clear Alarm is not generated from device
CSCvv53387	cedge is sending incorrect if index values for the sub-interfaces.
CSCvv54152	CDP on interfaces is not enabled when CDP is enabled globally on ASR Routers in controller mode
CSCvv58786	Connected route is not imported into OMP database unless flap interface with C8KV platform
CSCvv65659	Cisco IOS XE SD-WAN Software Privilege Escalation Vulnerability
CSCvv68635	Observed HTX core at tcpproxy_libuinet_pkt_process during longevity test
CSCvv69702	4451 : FTMD crash @ bfdmgr_session_get_from_record_index with traffic soak
CSCvv76523	Recursive configuration with privilege exec level <level> show dmvpn [detail|static]
CSCvv79072	25G license tags is retained and throughput throttled after upgrade from 17.3.1 to 17.3.2
CSCvv82949	C8500-12X4QC: Reload reason is not getting captured correctly after Kernal crash.
CSCvv84400	IR1101 - WP7607 modem is changing to down state after ping to enodeB
CSCvv91575	C1111-8P: NAT translations packet counter MIB OID counts unnecessary additional value
CSCvv92064	App-aware policy need to be honored when queuing is not set by localized policy
CSCvv92630	PKI http client fails to handle 1xx and 2xx responses
CSCvv99281	BQS crash on PPPoE session churn overnight
CSCvv99800	ASR 1000 FMANFP crashes during bootup with memory corruption
CSCvw01238	Enable AES encryption on cEdge and encrypt umbrella and zscaler secret/password

Caveat ID Number	Description
CSCvw02527	ASR 1000 NAT66 communication failure when change the NAT66 prefix configuration.
CSCvw06053	The CA certificate gets deleted after reboot in Cisco Catalyst 9800-CL Cloud Wireless Controller
CSCvw06287	IKEv1 mib statistics for Global Routing Table are incorrect if there are any IKEv2 sessions in fvrf
CSCvw11902	Passive FTP doesn't work with NAT
CSCvw13048	crash observed at NHRP while using summary-map
CSCvw20165	INTRED: Crash seen on BNG+NAT setup with scaled pools and "max-entries all-host "limit being hit
CSCvw21753	XE-SDWAN device would keep invalid IPv6 address in the tunnel to vManage and can not recover
CSCvw23041	Crash with high netflow traffic due to %CPPHA-3-FAILURE: R0/0: cpp_ha: CPP 0 failure Stuck Thread(s)
CSCvw23565	NAT pm entries get deleted after router reload in polaris_dev
CSCvw27787	NBAR not able to recognize application in a capwap-tunnel
CSCvw33950	C8300-1N1S-4T2X: QFP uCode crash @ ipv4_nat_create_out2in_session_entry with traffic soak
CSCvw34157	APPNAV CFT Crashes
CSCvw35840	Template attach failed with error: An element value is not correct : auto-bandwidth-detect.
CSCvw36514	cEdge crashes due to a large packet at vesen_ipsec_v4_input_get_vctrl_data
CSCvw36629	cEdge: NATed tuple flips for HSL deleted flow
CSCvw39383	CPP ucode crash with fw_base_flow_create
CSCvw46753	After reload cEdge cellular interfaces in shutdown state are brought up
CSCvw47800	HSL Export over VASI Interface causes Netflow v9 Template Flooding
CSCvw48800	unable to transfer 1500 byte IP packet when using BRI bundled Multilink
CSCvw48943	crypto ikev2 proposals are not processed separately
CSCvw50512	C8500-12X/C8500-12X4QC: Factory-reset doesn't format harddisk in 16GB/32GB/64GB variants
CSCvw52661	crash. seen during sh plat sof sdwan fo next-hop overlay id 0xf8000090
CSCvw54383	DPI flow telemetry generated by IOS-XE, for some flows tunnel identifiers are missing

Caveat ID Number	Description
CSCvw54521	Config-register IOS config CLI ignores bits corresponding to console speed w/o acknowledgment
CSCvw55030	Dynamic Nat pool "ip aliases" are not created on the device
CSCvw57860	Duplicate entries seen in MAC filter table.
CSCvw58560	FlexVPN reactivate primary peer feature does not work with secondary peer tracking
CSCvw59276	erspan classify ucode crash
CSCvw60359	cEdge-policy: set next-hop-ipv6 is not working next-hop-ip (ipv4) is working.
CSCvw61132	%PARSER-5-HIDDEN: Warning!!! ' resume server /connect telnet server' is a hidden command.
CSCvw61731	ASR 1000 router is not programming correct next-hop for the destination prefix.
CSCvw78062	C8500L-8S4X crashes when NAT sessions are removed
CSCvw87300	IP address not correctly in SIP traffic
CSCvx36763	Zone Based Firewall on cEdge router dropping web traffic with the reason Zone-pair without policy
CSCvx55296	CWMP: WANIPConnection.ExternalIPAddress sent in inform instead of WANPPPConnection.ExternalIPAddress
CSCvx57833	QFP crash due to IPv6 DNS ALG processing
CSCvx64846	"show sdwan policy" command cause device crash

Open Bugs for Cisco IOS XE Bengaluru 17.5

Caveat ID Number	Description
CSCvv74257	'sh plat CPU share' o/p prints incorrect percentage share values
CSCvw13682	L3 connected lite session not coming up , stuck in data-plane(qfp)
CSCvw56651	config-sync issue after enabling dmlog without rotation
CSCvw67366	ASR1002-X: Punt keepalive crashed due to bqs related interrupt
CSCvw69411	OC: unable to configure interface negotiation and speed via netconf rcp.
CSCvw87256	ASR 1000 cpp_cp_svr crash with frequent underlay route removal and tunnel source changed every 1 second
CSCvw89147	Crash at the moment of calculating tcp header
CSCvw91361	Crash when issuing "show crypto isakmp peers config"

Caveat ID Number	Description
CSCvw93769	Bias-free changes for CLI show mgcp srtp
CSCvw96723	CP process crashed while I95 driver was adding an IPC response to the receive ring
CSCvx02965	17.5-ASR1k-9X,6X,13RU: fsck for harddisk always fails with error Device Busy.
CSCvx08118	ASR1001-X: Bug to further address CSCvt08179 : QFP crash due to hardware interrupt
CSCvx32090	Port channel configuration triggers traceback
CSCvx32254	Memory leak in ess-cgm-class
CSCvx32807	False positive alarm: IOSXE_RP_ALARM-6-INFO: ASSERT CRITICAL Fan Tray Bay 1 Fan Tray Module Missing
CSCvx35902	fman_rp: qos_hqf [L:1.0, N:0x3485061e18] (0p, 0c) download to FP failed resulting in a crash.
CSCvx40718	Not able to remove FlowMonitor attached to intf when monitor is converted from unicast to multicast
CSCvx47010	Tunnel: CPP crashes at IPv4 tunnel decapsulation
CSCvx53063	IPsec crash. System couldn't resolve ipsec mapping.
CSCvx58180	can't ping vlan with "load-balance vlan" under 17.3.2
CSCvx59542	ASR1001-X upgrading throughput from 5G to 20G is consuming upgrade from 2.5G to 20G license
CSCvx59735	ASR 1000 ucode crash when sending SIP traffic to device while having a packet-trace configured
CSCvx59898	Bias-free changes for connection trunk CLI and show command
CSCvx60573	Memory leak in fman at the moment of getting routes
CSCvx63642	Can't allocate MAC address for port-channel interface on C1100TG series terminal server
CSCvx66807	REST virtual service crashes when traffic peaks and requires reload to restore
CSCvx72682	[DMM/SLM test issue] CFM crash when using physical port, DMM/SLM doesn't work on EVC
CSCvx74208	UDP port in IKE packets is not preserved with IKE preserve-port configured
CSCvx74212	IKEv1 IPSec CAC (Call Admission Control) counter leak leading to %CRYPTO-4-IKE_DENY_SA_REQ
CSCvx75330	fman_rp memory leak in acl_config_bind_v4_acl_message function.
CSCvx75352	CWMP port mapping description is lost after CPE reload

Caveat ID Number	Description
CSCvx77674	A router may crash when processing an NHRP packet
CSCvx79458	ISG: IPoE subscribers QOS not installed in the hardware after churn
CSCvx79581	%SCHED-3-THRASHING log observed after show cellular [int] drop-stats command.
CSCvx80677	ASR 1002-X: Seeing IPSEC-3-HMAC_ERROR: IPSec SA receives HMAC error
CSCvw90220	Crash at #12 0x00007f010f4cb9db in cpp_bqs_rm_yoda_get_flush_obj while subscriber bringup
CSCvw94434	BQS crash seen at cpp_qm_event_proc_defer_cb
CSCvw98579	BQS crash seen in 17.3 while bringing up 30k PPPOE sessions
CSCvx11702	C8500-12X4QC: Traffic drops on 10G interface with large packet size 9000bytes with High priority.
CSCvx26065	1006-X: Box rebooted due to ucode crash, with 2M CFLOW and 8K BFD sessions
CSCvx37388	DHCP relay- cEdge does not forward DHCP Offers correctly with IPv6 UnderLay
CSCvx69830	ASR 1000: BQS crash seen at cpp_qm_event_proc_defer_cb
CSCvx77587	AppQoE DRE monitoring graph, shows Optimized traffic is greater than Original traffic
CSCvx78054	tcp key chain not getting deleted from running config when it is used for SXP session bring up
CSCvx89710	SCEP: CA server fails to rollover CA certificate with error: "Storage not accessible"
CSCvy01097	Router may crash under ZBF configuration (cpp_cp_svr)

ROMmon Release Requirements

Use the following tables to determine the ROMmon version required for your Catalyst 8500 model:

Table 2: Minimum and Recommended ROMmon Releases

	DRAM	Minimum ROMmon	Recommended ROMmon
C8500-12X4QC & C8500-12X	16GB(default)	17.2(1r)	17.11(1r)
	32GB	17.2(1r)	17.11(1r)
	64GB	17.3(2r)	17.11(1r)
C8500-20X6C	All variants	17.10(1r)	17.10(1r)

C8500L-8S4X	-	17.10(1r) -	17.14(1r)* **Important** This version of ROMmon is only available with Cisco IOS XE 17.15.1a onwards

Note In case of C8500L-8S4X platform, the ROMmon image is bundled with the Cisco IOS XE software image which ensures that when the device is booted up, the ROMmon image is also automatically upgraded to the recommended version.

Table 3: What's New in the ROMMon Release

ROMmon Release for C8500-12X4QC, C8500-12X	Fixes
17.3(1r)	Supports 64GB DRAM for C8500-12X4QC & C8500-12X
17.10 (1r)	Added support for new platform C8500-20X6C
17.11(1r)	Fixed a issue in data wipe feature

ROMmon Release for C8500L-8S4X	Fixes
17.14(1r)	CSCwf98337 - Evaluation of C8500L-8S4X for Intel 2023.3 IPU and SMRAM vulnerabilities CSCwe21026 - Evaluation of C8500L-8S4X for Intel 2023.1 IPU and SMM vulnerabilities

Related Documentation

- Hardware Installation Guide for Catalyst 8500 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8500L Series Edge Platforms
- Smart Licensing Using Policy for Cisco Enterprise Routing Platforms
- Software Configuration Guide for Catalyst 8500 Series Edge Platforms

© 2020 Cisco Systems, Inc. All rights reserved.