Release Notes for Cisco Catalyst 8500 Series Edge Platforms, Cisco IOS XE Dublin 17.11.x

First Published: 2023-04-06

Full Cisco Trademarks with Software License

About Cisco Catalyst 8500 Series Edge Platforms

Note Cisco IOS XE Dublin 17.11.1a is the first release for Cisco Catalyst 8500 Series Edge Platforms in the Cisco IOS XE Dublin 17.11.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
- C8500-20X6C

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.

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.

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 http://www.cisco.com/go/cfn. An account on cisco.com is not required.

New and Changed Hardware Features

Table 1: Hardware Features

Feature	Description
Cisco Catalyst 8500-20X6C Edge Platform	The Cisco Catalyst 8500-20X6C Edge Platform, as part of the Catalyst 8500 series of routers, is available from Cisco IOS XE Dublin 17.10.x. The C8500-20X6C router is designed to provide high-speed connectivity and advanced security features for enterprise networks. For more information on this, refer to the Cisco Catalyst 8500 Series Edge Platforms Hardware Installation Guide and Software Configuration Guide.

New and Changed Software Features

Table 2: Software Features

Feature	Description
Support for RAR PPPoE IPv6 Multicast	This feature provides support for IPv6 multicast in PPPoE-based Radio Aware Routing (RAR) networks.
Attaching Extended Color Communities to BGP VRF	This feature introduces new methods of attaching extended color communities to a prefix. A color community is an indicator of the bandwidth or latency level of the traffic sent to the prefix. You can attach the the extended color communities to the prefix in the following ways: VRF export coloring, VRF import coloring, Route Redistribution coloring into BGP and Neighbor inbound coloring.
Upgrade in IPsec Tunnel Scaling Limits for High-End Aggregation	IPsec FlexVPN tunnel scale is improved for QFP 3.0 based Catalyst 8500 platforms
Support for Radio Aware Routing (RAR) and Dynamic Link Exchange Protocol (DLEP)	This feature enables Radio-Aware Routing (RAR) support on Cisco Catalyst 8000 Edge Platforms. RAR is a mechanism that uses radio signals to interact with the routing protocol OSPFv3 to signal the appearance, disappearance, and link conditions of one-hop routing neighbors. Cisco Dynamic Link Exchange Protocol (DLEP) is the latest protocol in the RAR family. DLEP provides a bidirectional, event-driven communication channel between the router and the modem/radio to facilitate communication of changing link characteristics.

Feature	Description
Device Telemetry	This functionality enables collection of anonymous usage telemetry data for Cisco products, which helps in continuous product improvements. From Cisco IOS XE 17.11.1a, this functionality is enabled by default.
Replication of Broadcast, Unknown-unicast, and Multicast Traffic	With this enhancement, the multi-destination Layer 2 broadcast, unknown-unicast, and multicast (BUM) traffic in an EVPN VXLAN network is replicated through a multicast group in the underlay network and forwarded to all the endpoints of the network.
MAC and IP Addressing Learning from a Static ARP Alias Entry	This enhancement allows you to configure an EVPN VXLAN network to learn an EVPN MAC address and IP binding from a static Address Resolution Protocol (ARP) alias entry. After learning the MAC address and IP binding, an EVPN Type-2 route is advertised across the EVPN network.
Deprecation of weak ciphers	The minimum Rivest, Shamir, and Adleman (RSA) key pair size must be 2048 bits. The compliance shield on the device must be disabled using the **crypto engine compliance shield disable** command to use the weak RSA key.

Resolved and Open Bugs for Cisco IOS XE 17.11.x

Resolved Bugs for Cisco IOS XE 17.11.1a

Bug ID	Headline
CSCwd47940	PMTU Discovery is not working after interface flap
CSCwd45402	MSR Unicast-To-Multicast not working if DST and SRC are the same in Service Reflect configuration
CSCwc79115	Commit failure notification and alarm from device
CSCwd16559	ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table
CSCwd67198	uCode crash seen on device after stopping NWPI trace
CSCwe28204	Control connection over L3 Tloc extension failing as no NAT table entry created
CSCwe22353	IpFormatErr drops on device when bridge-domain/EVC MAC learning limit is exhausted
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected
CSCwd89012	Tested flap-based auto-suspension - minimum duration value - no results as expected
CSCwe29430	Critical process fpmd fault on rp_0_0 (rc=134)
CSCwd87195	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.

Bug ID	Headline
CSCwd81357	QoS Classification not working for DSCP or ACL + MPLS EXP
CSCwc99823	fman crash seen in SGACL@ fman_sgacl_calloc
CSCwd71458	Outgoing number of bytes decrease in C8500L router' interface
CSCwd44439	Device crashing at fman_sdwan_nh_indirect_delete_from_hash_table
CSCwd34941	NAT configuration with no-alias option is not preserved after reload
CSCwc72588	Router should not allow weak cryptographic algorithms to be configured for IPsec
CSCwd25107	interface VLAN1 placed in shutdown state when configured with ip address pool
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature
CSCwd05356	Error %HW_FLOWDB-3-HW_FLOWDB_DBLINSTALL_FEATOBJ
CSCwe00946	Device crash after disabling endpoint-tracker on tunnel interfaces
CSCwe18058	Unexpected reload with IPS configured
CSCwd61255	Data plane crash on device when making per-tunnel QoS Configuration changes with scale
CSCwe01015	IKEv2/IPSec rekey failing when peer is behind NAT
CSCwd65945	LR Interface which has NAT enabled is chosen for webex traffic
CSCwe27241	NBAR classification error with custom app-aware routing policy
CSCwc37465	Unable to push no-alias option on static NAT mapping from management system
CSCwe19084	Traffic is not translated to the same global address though PAP is configured
CSCwc67625	OU field is deprecated from CA/B Forum certificate authorities
CSCwe33793	Memory allocation failure with extended antireplay enabled
CSCwe23276	Change in the IPsec integrity parameters breaks the connectivity
CSCwd46921	Device is not connecting
CSCwe34808	FMAN FP leak due to the punt-policer command
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through device
CSCwd30578	Wired guest client stuck at IP_LEARN with DHCP packets not forwarded out of the foreign to anchor
CSCwd84391	IP fragments incorrectly dropped due to reassembly timeout
CSCwe60059	Crash when using dial-peer groups with STCAPP
CSCwd15487	Kernel crash is observed when modem-power-cycle is executed
CSCwd67654	FnF stats are getting populated with unknown in egress/ingress interface in vpn0
CSCwd38943	KS reject registration from a public IP
CSCwb59113	BFD session gets NAT translated with static ip over dialer interface
CSCwe03614	MAC address of ATM interface is not included in Inform message

Bug ID	Headline
CSCwb46968	PPPoE commands are removed from ethernet interface
CSCvy14316	MPLS VPN traffic dropped due FDB OOM with cause FIAError under scale flow number
CSCwe69783	Device loses its config during a triggered resync process if lines are in an off-hook state
CSCwd71586	BFD sessions flapping on an interface with SYMNAT may lead to IPSec crash
CSCwe41946	DTMF is failing through IOS MTP during call on-hold
CSCwd06923	Stale IP alias left after NAT statement got removed
CSCwc48427	BFD issues with clear_omp -> non-PWK + non-VRRP scenario only
CSCwd28593	Control connection flap after shutting down
CSCwd90168	Unexpected reload after running **show voice dsp** command while an ISDN Call disconnects
CSCwe32862	Router IOS-XE crash while executing AES crypto functions
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwd68994	ISAKMP profile doesn't match as per configured certificate maps
CSCwd79572	FW policy with app-family rule with FQDN causes traffic drop for other sequences
CSCwe91988	Need to disable CSDL compliance check for NPE images

Open Bugs for Cisco IOS XE 17.11.1a

Bug ID	Headline
CSCwd42523	Same label is assigned to different VRFs
CSCwd45508	Device does not form BFD across serial link when upgrading
CSCwe19394	Device may boot up into prev_packages.conf due to power outage
CSCwe49509	Some BFD tunnel went down after migration
CSCwe37123	Device uses excessive memory when configuring ACLs with large object groups
CSCwe39157	Memif channels are missing causing SC-SN state down
CSCwe09298	Device sees the increase of input errors without any other specifc errors increasing under sh int
CSCwe18276	Route-map not getting effect when its applied in OMP for BGP routes
CSCwe40024	98% memory utilization for device
CSCwe35574	DPDK RX buffer is getting corrupted causing crash
CSCwd68111	Device object group called in ZBFW gives error after upgrade
CSCwe39011	GARP on port up/up status from Catalyst 8300 and Catalyst C8500L device is not received by remote peer device
CSCwe49684	BFD sessions keeps flapping intermittently
CSCwe52971	BFD tunnels remain in down state

ROMmon Release Requirements

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

Table 3: 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	-	17.8(2r) - available from Cisco IOS XE 17.9.1a release	-
	-	17.10(1r)- available from Cisco IOS XE 17.10.1a release	-

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 4: ROMmon Release per Platform

C8500-12X4QC & C8500-12X	17.2(1r)
	17.3(1r)
	17.11(1r)
C8500-20X6C	17.10(1r)
C8500L-8S4X	17.8(2r)
	17.10(1r)

Table 5: 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

ROMmon Release for C8500-12X4QC, C8500-12X	Fixes
17.11(1r)	Fixed a issue in data wipe feature

ROMmon Release for C8500L-8S4X	Fixes
17.10(1r)	CSCwa41877 - Fixes for Intel 2021.2 IPU CSCwb67177 - Fixes for Intel 2022.1 IPU CSCwb60723 - Fixes for CPU temperature CSCwb60863- Fixes for TAM_LIB_ERR_WRITE_FAILURE error

Related Documentation

- Hardware Installation Guide for Catalyst 8500 Series Edge Platforms
- Hardware Installation Guide for Catalyst 8500L Series Edge Platforms
- Smart Licensing Guide for Access and Edge Platforms
- Software Configuration Guide for Catalyst 8500 Series Edge Platforms

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.