Release Notes for Cisco Catalyst 8000V Edge Software, Release 26.2.x

Contents

Cisco Catalyst 8000V Edge Software, Release 26.2.x

Cisco 26.2.1 is the first release for Cisco Catalyst 8000V Edge Software in the Cisco IOS XE 26.2.x release series.

New software features

This section provides a brief description of the new software features introduced in this release.

New software features in Cisco IOS XE 26.2.1

Table 1. New software features for Cisco Catalyst 8000V Edge Software, Release 26.2.1

Product impact	Feature	Description
Hardware reliability	Resilient Infrastructure Changes	As part of Cisco's Resilient Infrastructure program and Cisco's commitment to secure infrastructure, this release includes additional changes aimed towards continuing to make Cisco IOS XE more secure by default. Note that some of these changes may require operational changes if you are not following secure best practices. This release includes the following changes: The RADIUS client appends the Message-Authenticator attribute (Attribute 80 HMAC-MD5) to all outgoing Access-Request packets to mitigate cryptographic forgery and Blast-RADIUS vulnerabilities (CVE-2024-3596). The RADIUS client drops incoming Access-Accept, Access-Reject, and Access-Challenge packets if the Message-Authenticator packet is absent or invalid. Ensure AAA servers (example, Cisco ISE) are configured to return Attribute 80. Outbound SSH connections enforce Trust-On-First-Use (TOFU). The device prompts to verify and store remote server host keys in the known-hosts database on first connection and validates against them on subsequent sessions. Proxy ARP is disabled by default across all routed interfaces, SVIs, and subinterfaces to reduce Layer 2 broadcast domains and prevent ARP spoofing. Configure the ip proxy-arp command explicitly if required. The embedded web server daemon is disabled by default on factory configurations to restrict unauthenticated management access. Web UI and RESTCONF require explicit enablement of the ip http secure-server command. The IOS XE device rejects unauthenticated NTP Mode 6 and Mode 7 control queries (monlist) to prevent NTP reflection and amplification DDoS attacks. Standard time synchronization (Modes 3 and 4) is unaffected. Warning messages are emitted on the console and logged to syslog whenever legacy insecure protocols (telnet, ftp, tftp, http) are enabled in the configuration. Real-time tracking of active insecure services is published to the operational database (operDB) and YANG data models, allowing management controllers (such as Cisco Catalyst Center) to monitor security compliance.

Product impact	Feature	Description
		For more information, refer Resilient Infrastructure.
API experience	IPv6 day-0 onboarding with DHCPv6 prefix delegation	Adds DHCPv6-PD as an IPv6 address-discovery option in the ZTP/PnP workflow for Cisco IOS XE Catalyst SD-WAN devices. ZTP runs IPv4 and IPv6 address discovery in parallel, and IPv6 discovery can use stateful DHCPv6, SLAAC, or DHCPv6-PD.
Upgrade	Secure Router NGFW	Secure Router NGFW introduces Cisco Catalyst NGFW, a new security-application container for supported Cisco Catalyst 8000 Series Secure Routers. In Cisco IOS XE Catalyst SD-WAN Release 26.2.1 and Cisco Catalyst SD-WAN Manager Release 26.2.1, the feature provides workflows to install Catalyst NGFW and migrate supported settings from NGFW V1 Engine (UTD) to NGFW V2 Engine (Catalyst NGFW). IPS and IDS retain their core detection and prevention behavior while using Talos Lightweight Security Package (LSP) content. The release also adds Encrypted Visibility Engine (EVE) for encrypted-flow analysis without payload decryption and introduces Snort ML inspection for supported threats. Catalyst NGFW replaces the UTD community/subscriber signature-package workflow with independently managed LSP and Vulnerability Database (VDB) packages. LSP contains Talos rules and detectors; VDB provides application, fingerprint, and enrichment information.
Ease of use	Port settings for speed, duplex, and auto-negotiation	Configures speed, duplex, and negotiation auto in a single command.
Software Reliability	Packet-Order Preservation during Tunnel Underlay Reassembly	Cisco IOS XE 26.2.1 introduces Packet-Order Preservation during tunnel underlay reassembly that ensures a tunnel endpoint forwards completed, reassembled packets from the same traffic flow in correct order. The feature operates with packet reassembly boost mode on supported Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager.
Ease of use	Discontiguous Subnet Mask Support for IPv4 Network Object Groups	Adds support for discontiguous subnet mask entries in IPv4 data prefixes and IPv4 network object groups used by NGFW Policy. You can use discontiguous subnet mask entries in IPv4 source and destination match conditions, rule sets, object groups, and deploy-time data prefix variables.
Ease of setup	EVPN VPWS over SRv6	This feature adds support for EVPN VPWS over SRv6 transport. EVPN VPWS uses EVPN signaling and SRv6 encapsulation to provide point-to-point Layer 2 VPN service between provider edge devices.
CUBE Features		
Security	Automatic conversion of password formats into secure types	Starting with Cisco IOS XE 26.2.1, it is recommended to use Type 6 (AES) for provisioning all credentials to comply with security standards. CUBE supports auto-conversion of Type 0 or Type 7 to reversible Type 6 encryption.
Security	Security warnings for non-secure protocols	Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used. For CUBE, use secure alternatives such as HTTPS, SFTP, or SCP.

Changes in behavior

This section provides a brief description of the behavior changes introduced in this release.

Changes in behavior in Cisco IOS XE 26.2.1

Table 2. Behavior changes for Cisco Catalyst 8000V Edge Software, Release 26.2.1

Description	Behavior changes
The ip nat translation nonpat-timeout keyword allows configuring a timeout from 0 to 536870 seconds or setting it to never.	Refer to the ip nat translation (timeout) command.
DHCP relay is always enabled by Cisco IOS and provide status verification for cellular modems	Refer to the Configuring the DHCP Client section.
Certificate hexadecimal data appears under crypto pki certificate chain in show running-config by default. Starting with Cisco IOS XE Release 26.2, configure the crypto pki certificate hidehex command hides certificate hexadecimal data from show running-config output while retaining the certificate chain and entry.	Refer to the Certificate Hexadecimal Data Output Example.
The procedure for configuring a trustpoint for EST is updated.	Refer to the Configure a trustpoint for EST section.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Resolved issues in Cisco IOS XE 26.2.1

Table 3. Resolved issues for Cisco Catalyst 8000V Edge Software, Release 26.2.1

Bug ID	Description
CSCwt10887	SDWAN edge router device crashed after attempting to push a config group
CSCwv02836	SDWAN edge router: upgrade process may report enormous " Required space"
CSCwv02835	[IOS XE] 6VPE: Locally terminated IPv6 traffic fails over BDI interface
CSCws50867	17.18/26.1: Tracker probe id set to 0 while changing Invalid DNS endpoint to endpoint-ip
CSCwt54094	C8kv queue-limits are not adjusted in the policy-map after hsec license is installed.
CSCwu03035	SDWAN edge router: UTD may silently drop large fragmented RADIUS packets
CSCwv34598	SDWAN edge router Router Reset due to PuntInject Keepalive Timeout (No Ucode File Generated)
CSCwu83262	L2TPv3 xconnect session fails to establish when the traffic traverses through IPsec tunnel interface.

Bug ID	Description
CSCwt79827	IOS-XE not parsing transform payload with unknown attributes
CSCwu03372	Unexpected reload due to ftmd fault on SDWAN edge router with On-Demand Tunnels
CSCwv23165	BFD echo packet counters report a fixed 2:1 tx/rx ratio (false 50% packet loss) on all tunnels after enabling Enhanced Application Aware Routing
CSCwu27070	Unexpected Reload in CPP Server (cpp_sp_svr) Code
CSCwt67685	SD-WAN Edge: Periodic Service Restart May Generate Crash Files
CSCwu39202	SDWAN edge router : Power reset during cEdge boot causes router to enter ROMMON
CSCwt47734	Endpoint-tracker HTTP probe sends IP address instead of FQDN in 17.15
CSCwu21490	Kernel Core Files Deleted From Flash When Incomplete Admin Tech is Generated
CSCwv60786	Intermittent issue with RRI being lost on the Flex Hub
CSCwr02102	Router intermittently loses ip address dynamically assigned to tunnel interface
CSCwr60310	SDWAN Template push or CLI config update fails due to the duplication of VTY or Async lines in the configuration
CSCwu49029	Unexpected reload on CGM (Class-Group Manager) when updated
CSCwt75037	Device in controller mode crashes with Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)
CSCwu49303	Memory Leak in cpp_sp_svr due to Classification Objects
CSCwu61766	SDWAN edge router OMPD crash on malformed SD-WAN identity IP-to-user update from vSmart pxGrid integration
CSCwt70932	BFD session establishment failed due to ARP resolution failure.
CSCwt44263	VPN ID is not maintained after UTD feature causing ZBFW to evaluate against incorrect policy
CSCwt66413	ncsshd process fails to terminate after " no netconf" and netconf refuses connection
CSCwt56693	L2TP: Seeing " protocol l2tpv2 L2TP_CLASS_011" config getting lost with clear ppp all cli
CSCww00071	Router crashed while decrypting NAT-T IPsec traffic with CTS SGT enabled
CSCwv25887	High QFP utilization due to NAT translation timeout and concurrent translation creation causing allocator contention
CSCwt84502	Critical Process cpp_ha_top_level_server crash (rc=69) Crash after adding zone based firewall setup configuration on the router
CSCwu53168	SDWAN edge router upgrade fails with " timeout" when confd Phase 0 failure
CSCwt17412	Sessions appear as two unidirectional records instead of one bidirectional flow

Bug ID	Description
CSCwv08826	SDWAN edge router : BOW in EAAR not working when tunnels are outside SLA and outside variance
CSCwv52757	UDP packets multicast destination not seen on FIA-Trace nor EPC over xconnect
CSCws68686	Application Policy: IPv6 BGP Neighborship Fails When Using Basic Policy with Default Drop Action
CSCwt16689	QFP command displays incorrect App-Probe-Class (APC) queue assignment
CSCwv61185	C8000V vdaemon may flap SD-WAN control connections with HWCERTREN when multiple vManage-signed edge certificates have identical Not Before timestamps.
CSCwv69412	1.3.6.1.4.1.9.9.86.1.6.4.1.13.x value keep stale value until execute show dspfarm all
CSCwu67470	Unexpected reload on SDWAN edge router device after changing secuity policy to none on template
CSCwt97049	Buffer Overflow in Domain Name Pattern Handling Causes Pointer Corruption and System Crash
CSCwt46462	Enable alerts for the EC genet server (Transform) dying or timing out
CSCws66553	fpmd crash seen with 17.12.6B respin image with longer soak + clear sdwan omp events
CSCwt45748	Crash while processing packet in AppNav Tunnel
CSCwu10100	Endpoint tracker is unable to determine next-hop for DNS name resolution from Dialer interface
CSCwr49368	SSE Tunnels with Cisco Secure Access are stuck in SD-WAN Configuration Database
CSCwu02842	Unexpected reload due to race condition in QoS service group configuration
CSCwt92911	Crash in OMP process during end point tracker teardown
CSCwv42272	NULL Dereference in NHRP MIB
CSCws98086	Update " reason for state change: MAX" in BFD Syslog
CSCwt25903	Not able to disable " log" feature in NGFW Policies vManage for " Drop" rules.
CSCwv71880	SD-WAN redirect-dns Destination NAT session collides with SIG tunnel IKEv2 control plane traffic
CSCws95879	ICMP TTL Expired packet sent via incorrect VRF
CSCwu76495	SDWAN: Crash while updating Adaptive QOS Session Policy due to minimal traffic size
CSCwu86821	Service-chain config modify to local svc-chain failed to delete old TLOC list action leading to packet drops
CSCwu31509	Secondary OU is not generated in CSR for SD-Routing(Autonomous mode) devices

Bug ID	Description
CSCwv09160	HTTP SIG Tracker trying to resolve endpoint-api-url IP address via DNS after upgrade to 17.15.05
CSCwt94337	cpp_cp_svr crashes with SIGSEGV whle printing packet trace data
CSCwu51162	Unexpected reload on router in SDWAN CCE (Classifier and Classification Engine)
CSCwv73701	Packet reordering observed when application performance-monitor service policy enabled
CSCwu34418	QFP crash with qfp-ucode and cpp_cp_svr cores
CSCwu53407	Standalone endpoint-tracker UP recovery syslog missing intermittently on SDWAN edge router
CSCwu35982	Router unexpectedly reloads after IKEv2 operations
CSCwr76176	BFD SD-WAN PMTUD: PMTU Converges Unexpectedly to 970 Bytes After dbg2:1 Event
CSCwu47545	Ucode Code Crash while Printing Log for FW Drop for Packet with Invalid Header
CSCwv67035	Ikev2 PPK Unable To Switch Back to PSK When 'Required' Is Used in Keyring
CSCwt56693	L2TP: Seeing " protocol l2tpv2 L2TP_CLASS_011" config getting lost with clear ppp all cli

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Open issues in Cisco IOS XE 26.2.1

Table 4. Open issues for Cisco Catalyst 8000V Edge Software, Release 26.2.1

Bug ID	Description
CSCww05599	Unexpected reload due to NAT pool exhaustion
CSCwv84068	17.12.6 likely change in the SDWAN edge router code is causing the control connections failing to come up
CSCww02502	Umbrella tunnels down, reporting cdb-validate-info failed state with 401 authentication error.
CSCwv71872	CoR-SaaS custom-app endpoint-url probing on free configurable port
CSCwv61920	Standby RP Rebooting Frequently After Applying Static Named NAT Entry
CSCwv86632	IOSd crash in " Open DNS Dev-Reg" process on 17.12.6 despite CSCwp09231 fix (Umbrella device-registration UAF during config churn)

Bug ID	Description
CSCwv65418	SDWAN ICMP interface tracker goes up everytime the router resolves the DNS-name configured
CSCwv91764	CSCwv91764 - 26.2 Zscaler SSE GRE:The Public IP address for every tunnels entered on the vManage doe
CSCww20413	Update outdated GeoDB in 17.18.x
CSCwu24210	SDWAN edge router .sdwaninstaller accounting for rollback files in disk space calculation
CSCww00586	UTD context with no inspection features enabled stays in Divert mode; traffic black-holed at memif
CSCwv80846	IOSd crash in router_init due to stale PDB pname during routing process creation
CSCww00540	SDWAN edge router - 17.12.8 endpoint-tracker reports all shared-tracker tunnels Down when one tunnel fails DNS
CSCwv98085	SDWAN 17.18.2- Cli config push fails, SDWAN edge router displays Error: application communication failure> while running " show sdwan running"

Related resources

List the related content, matrices, videos, and tools.

- Cisco Catalyst 8000V Edge Software Product Page
- Cisco Catalyst 8000V Edge Software Data Sheet
- Cisco Catalyst 8000V Edge Software Installation And Configuration Guide
- Cisco Catalyst 8000V Edge Software High Availability Configuration Guide
- Troubleshooting Guide for Cisco Catalyst 8000V Edge Software
- Configure Licenses and Throughput for Cisco Catalyst 8000V Edge Software

Legal information