
# ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco Aggregation Services Router 1000 Series (ASR1K) Cisco Catalyst 8200, 8300, 8500 Series Edge Routers (Cat8K) running IOS-XE 17.18

---

**Maintenance Update of Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Catalyst 8200, 8300, 8500 Series Edge Routers (Cat8K) running IOS-XE 17.18**

**Maintenance Report Number:** CCEVS-VR-VID11642-2025

**Date of Activity**: 12 December 2025

**References:**

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016.
- Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Catalyst 8200, 8300, 8500 Series Edge Routers (Cat8K) running IOS-XE 17.18, Impact Analysis Report - Update IOS-XE 17.15 to 17.18, Version: 0.3, December 10, 2025.

**Evaluated TOE**

- **VR Title:** Validation Report for the Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Catalyst 8200, 8300, 8500 Series Edge Routers (Cat8K) running IOS-XE 17.15 Version 1.0, September 29, 2025.
- **VR Report #: CCEVS-VR-VID11642-2025**
- **VR Version** – 1.0
- **VR Date** –September 29, 2025

**Current AM TOE Updated**

- **ACMR Title** – ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco Aggregation Services Router 1000 Series (ASR1K) Cisco Catalyst 8200, 8300, 8500 Series Edge Routers (Cat8K) running IOS-XE 17.18
- **ACMR Report #: CCEVS-VR-VID11642-2025**
- **ACMR Version** – 1.0
- **ACMR Date** – December 11, 2025

**Documentation Updated**:

| CC Evidence | New CC Evidence | Change Summary |
|---|---|---|
| Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Catalyst 8200, 8300, 8500 Series Edge Routers (Cat8K) running IOS-XE 17.15 Security Target, Version 1.2, September 24, 2025 | Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Catalyst 8200, 8300, 8500 Series Edge Routers (Cat8K) running IOS-XE 17.18 Security Target, Version 2.0, October 10, 2025. | Updated to reflect IOS-XE version 17.18 software version number. |
| Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Catalyst 8200, 8300, 8500 Series Edge Routers (Cat8K) running IOS-XE 17.15 Operational User Guidance and Preparative Procedures, Version 1.0, September 11, 2025 | Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Catalyst 8200, 8300, 8500 Series Edge Routers (Cat8K) running IOS-XE 17.18 Operational User Guidance and Preparative Procedures, Version 2.0, October 10, 2025. | The CC Configuration Guides were updated to IOS-XE version 17.18. |

**Assurance Continuity Maintenance Report:**

Cisco Systems Inc. submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 10 October 2025. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence consists of the Security Target, Administrative Guidance, and the IAR. The ST and the Administrative Guidance documents were updated.

**Product Updates:**

All changes to the product were new feature enhancements, bug fixes. and CVE vulnerability patches. These changes have been assessed as minor. These enhancements do not affect the security functionality or claims of the previously evaluated TOE. New features and bug fixes are summarized in Appendix A and B.

**TOE Environment:**

There are no updates to operational environment components identified. The TOE environment is consistent with the validated results from the previous evaluation.

**Regression Testing:**

During development of a new IOS-XE version, there are various tests performed to ensure the product performs as expected. Bug fixes and new features are tested to ensure the feature works as expected or the fix was effective. Additionally, regression testing, using pre-defined test cases, is performed to ensure that overall product performs as expected, in essence ensuring existing features and functionality

from previous versions was not broken in the development of the latest version. Based on the bug testing and regression testing, Cisco believes the product behaves as expected.

**Assurance Coverage**

Having reviewed new features, vulnerability fixes, and bug fixes, Cisco has found no evidence that the newer version of the IOS-XE software had any changes to an SFR or SAR therefore regression testing was not required for the SFRs and SARs.

**NIST Certificates:**

The updates made to the TOE have not changed the cryptographic modules algorithm implementation nor their tested operational environment, so there is no impact to the CAVP certificates.

**Vulnerability Assessment:**

An updated vulnerability analysis was performed on October 10, 2025, December 5, 2025, and again on December 10, 2025, using the original search terms. 23 CVEs were found. The Vendor fixed all of these vulnerabilities with patches. There are no residual vulnerabilities in the new version of the product.

**Conclusion:**

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. No functionality, as defined in the SFRs, was impacted, and none of the product changes and vulnerability updates affected the security functionality or the SFRs identified in the Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.

# 1 Appendix B – New Features

The following new features were introduced into IOS-XE 17.18 since the certification of the IOS-XE 17.15 version. The new features were analyzed and determined to have no security relevance or fell out of the scope of evaluated functionality. The table lists and describes each feature and provides supporting rationale.

**Table 1. Non-Security Relevant New Features**

| Feature | Description | Rationale |
|---|---|---|
| Disablement of Weak SSH Algorithms | From Cisco IOS XE 17.16.1a, the ssh-rsa algorithm is disabled by default on port 22 to improve security. | The disabling of the weak ssh-rsa algorithm strengthens cryptographic security by default. This change does not negatively impact TOE security functions. |
| Monitoring Crypto VPN Solutions on SD-Routing Devices | If you have configured crypto VPN solutions such as DMVPN, FlexVPN or Layer 3 VPNs on SD-Routing devices, you can use Cisco Catalyst SD-WAN Manager to visualize the VPN solution deployed in the network and observe the functioning of the devices using various states, stats, charts and events.Having high visibility into the network can help identify errors in real time therefore reducing the network down time. | Monitoring enhancements are administrative/observability functions and do not alter or impact TOE security functions. |
| Monitoring Application Performance on SD-Routing Devices | In Cisco IOS XE 17.16.1a, you can now monitor TCP and RTP traffic on DMVPN tunnels for IKEv2 traffic using Application Response Time (ART) monitor and Media monitor respectively. This functionality is only supported on DMVPN tunnels with IKEv2 encryption. | Application performance monitoring is optional and informational only. It does not impact TOE security functions. |
| Enhanced support for binary tracing | From Cisco IOS XE 17.16.1a onwards, you can retrieve events sent to the IOS process in the binary trace using the show logging process IOS module nhrp command, without enabling DMVPN event tracing. | Enhancements to binary tracing are diagnostic and not related to TOE security functions. |
| Support for Enrolment over Secure Transport | From Cisco IOS XE 17.16.1a onwards, you can use HTTP-based authentication for EST Client Support, using the enrollment http username command. | Certificate enrollment using EST is not included in the evaluated configuration. Therefore, this enhancement does not impact TOE security functions. |
| Enhancement to the show cellular 0/x/0 connection command | From Cisco IOS XE 17.16.1a, the output for the show cellular 0/x/0 connection command includes Access Point Name (APN), and Cellular Link Uptime parameters. | Enhancements to show commands are informational only and do not impact TOE security functions. |
| Asymmetric carrier delay | From Cisco IOS XE 17.16.1a, asymmetric carrier delay is supported on Cisco Catalyst 8500 Series Edge Platforms. | This is a performance/latency feature and does not affect TOE security functions. |
| Enhancements to the show power command | From Cisco IOS XE 17.16.1a, two new keywords detail and history) are introduced for the show power command. The detail keyword provides power usage information for each component, and the history keyword provides the power consumption history for the device. | Enhancements to show commands are informational only and do not impact TOE security functions. |
| Enhancements to Segment Routing over IPv6 Dataplane | From Cisco IOS XE 17.16.1a, Segment Routing over IPv6 dataplane supports these functionalities: eBGP Inter-AS, PCE-Delegated Path Computation, Enhancements to OAM Traffic Engineering | Enhancements to routing protocols do not impact TOE security functions. |

| | | |
|---|---|---|
| Product Analytics for routers | Product Analytics refers to the collection of product telemetry such as product performance and resource usage information directly from IOS-XE-based routing platforms. From Cisco IOS XE 17.18.1a release, Product Analytics is enabled by default when you start your router. Use this functionality to gain data insights such as product performance, feature consumption, and the licensing types that suit your requirements best. | Product analytics is for operational telemetry only. Since it is not part of the evaluated configuration, this feature does not impact TOE security functions. |
| MVPN Ingress Replication (IR) over SRv6 | This feature enables the transport of IPv4 Multicast traffic across an SRv6 network. It simplifies multicast deployment by using the existing SRv6 unicast infrastructure as the underlay. With this feature, the ingress PE router receives multicast traffic and creates a separate unicast SRv6-encapsulated copy for each egress PE router in the multicast group. | Multicast and SRv6 enhancements are outside the evaluated configuration. Therefore, this feature does not impact TOE security functions. |
| SRv6 Path MTU Discovery | This feature introduces a mechanism to determine the maximum transmission unit (MTU) for packets traversing an SRv6 underlay network. It ensures efficient packet forwarding by preventing fragmentation and packet drops, thereby allowing network devices to dynamically adjust packet sizes to avoid exceeding link MTU limits. The system relays ICMP Packet Too Big (PTB) messages from the SRv6 underlay to the IPv6/IPv4 overlay network, supporting both Transit-node and Headend-node PTB relay methods. | Enhancements to SRv6 forwarding are operational and do not impact TOE security functions. |
| SRv6 Flex-Algo with TI-LFA and uLoop Avoidance | From Cisco IOS XE 17.18.1a, Flexible Algorithm enhances SRv6 by including functions like Topology Independent Loop-Free Alternate (TI-LFA) and microloop (uLoop) avoidance. This feature improves network resilience and efficiency. | Enhancements to SRv6 forwarding are operational and do not impact TOE security functions. |
| Product Analytics for routers | Product Analytics refers to the collection of product telemetry such as product performance and resource usage information directly from IOS-XE-based routing platforms. From Cisco IOS XE 17.18.1a release, Product Analytics is enabled by default when. Use this functionality to gain data insights such as product performance, feature consumption, and the licensing types that suit your requirements best. | MAP-T enhancements are protocol transition features and do not impact TOE security functions. |

| | | |
|---|---|---|
| MAP-T Border Router (BR) Enhancements | The Cisco IOS XE 17.18.1a release supports several enhancements to the MAP-T Border Router, an important component in facilitating IPv4 packet transmission over IPv6 networks. These improvements include enhanced support for fragmented ICMP packets during IPv4 to IPv6 transition, robust support for hairpin traffic between devices, and reliable handling of fragmented UDP packets with a checksum value of 0. These enhancements also provide service providers with a more comprehensive and resilient solution for maintaining essential IPv4 connectivity during the transition to an all-IPv6 environment. | MAP-T enhancements are protocol transition features and do not impact TOE security functions. |

# 2 Appendix B – Bug Fixes

The following are bugs fixed in IOS-XE 17.18 since the certification of the IOS-XE 17.15 version.

**Table 2. Non-Security Relevant Fixes for Bug Fixes**

| Cisco Identifier | Title/Description | Rationale |
|---|---|---|
| CSCwo84352 | Segmentation fault on the sessmgrd process | The fix corrects an internal process stability issue. It has no direct impact to any TOE Security Function (TSF). It only ensures the product functions as expected. |
| CSCwo19997 | QFP crash with stuck threads while attempting to lock cft policy under autonomous mode | The fix corrects an internal platform process issue. It has no direct impact to any TSF. |
| CSCwn99822 | Large number of BFD sessions stuck due to out of window drops reported with control connections NAT flaps | Bidirectional Forwarding Detection (BFD) is not included in the CC evaluated configuration. Therefore, updates to BFD are not applicable. |
| CSCwn60316 | "cpp-mcplo-ucode" crashes in device | The fix corrects a microcode crash. It has no direct impact to any TSF. |
| CSCwm62981 | Device crashes with PKI "revocation-check ocsp none" enabled | OCSP-based PKI revocation checking is not included in the CC evaluated configuration. Therefore, updates to OCSP are not applicable. |
| CSCwn52179 | Traffic with TTL 2 is punted to CPU when CEF holds MPLS labels set to none | MPLS is not included in the CC evaluated configuration. Therefore, updates to MPLS are not applicable. |
| CSCwo66822 | Device reloaded with reason: Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69) | The fix corrects a platform HA process fault. It has no direct impact to any TSF. |
| CSCwo59694 | YANG: Unable to deploy 'aaa accounting network' command | YANG/NETCONF management models are not included in the CC evaluated configuration. Therefore, updates to YANG are not applicable. |
| CSCwp12923 | IKEv2 fails to parse certain route-set prefix Cisco VSA attributes from Radius server | Vendor-specific RADIUS VSAs are not included in the CC evaluated configuration. Therefore, updates to VSAs are not applicable. |
| CSCwi44116 | IOS-XE reboot after change telemetry subscription update-policy from periodic to on-change | Telemetry is not included in the CC evaluated configuration. Therefore, updates to telemetry are not applicable. |
| CSCwo42107 | Device crashes when applying a service-policy to a PO interface used as tunnel source | QoS and service-policy behavior are not included in the CC evaluated configuration. Therefore, updates to QoS/service-policy are not applicable. |
| CSCwo90396 | Serial interface configuration lost after reload | The fix corrects Serial interface handling fault. It has no direct impact to any TSF. |
| CSCwm33545 | FlexVPN - IP address assigned to spoke changes to unassigned | FlexVPN is not included in the CC evaluated configuration. Therefore, updates to FlexVPN are not applicable. |
| CSCwk53854 | CLNS neighbors go down with MTU set and MACsec enabled | This defect affects CLNS neighbor discovery when MTU is constrained but does not alter MACsec cryptographic enforcement, replay protection, or MKA key lifecycle. Therefore, no impact to TSF claims. |
| CSCwn02485 | Fragmented UDP SIP packets dropped on PE with IpFragErr on IP VFR and MPLS enabled tunnel interface. | MPLS and SIP/VoIP are not included in the CC evaluated configuration. Therefore, updates to MPLS/VoIP are not applicable. |
| CSCwp02391 | Administratively shutdown ports are reenabled after core isolation recovery (WAN link recovered) | The fix corrects port state recovery. It has no direct impact to any TSF. |
| CSCwo15543 | Standby device reloads after upgrade | HA redundancy behavior is not included in the CC evaluated configuration. Therefore, updates to HA are not applicable. |
| CSCwn62695 | KMI messages introducing a crash while enabling debug. | Debug/logging processes are not TSF claims. Therefore, no CC impact. |
| CSCwn03824 | Memory leak in CCSIP_SPI_CONTROL and dead processes | VoIP/SIP stack is not included in the CC evaluated configuration. Therefore, updates to VoIP/SIP are not applicable. |
| CSCwo05166 | Memory leak on chunk manager via DBAL EVENTS process | The fix corrects memory handling. It has no direct impact to any TSF. |
| CSCwo09168 | Devices crashed due to critical process vip_confd_startup_sh fault | The fix corrects an internal configuration daemon crash. It has no direct impact to any TSF. |

| Cisco Identifier | Title/Description | Rationale |
|---|---|---|
| CSCwn91302 | Device does not retain dscp markings when using mpls on tunnel and qos on underlay interface | MPLS and QoS are not included in the CC evaluated configuration. Therefore, updates to MPLS/QoS are not applicable. |
| CSCwn06900 | Segfault in events | The fix corrects an event handler crash. It has no direct impact to any TSF. |
| CSCwn13851 | Device reports error logs | Logging issues outside TSF scope. Therefore, no CC impact. |
| CSCwm61335 | ID manager runs out of IDs, memory leak when using CTS | Cisco TrustSec is not included in the CC evaluated configuration. Therefore, updates to TrustSec are not applicable. |
| CSCwn92976 | PPP is not establishing when l2tp over ipsec | L2TP over IPsec is not included in the CC evaluated configuration. Therefore, updates to L2TP are not applicable. |
| CSCwn92855 | Breakout port fails to initialize | Breakout/PHY features are not included in the CC evaluated configuration. Therefore, updates to breakout ports are not applicable. |
| CSCwo66011 | Config parser issue for NAT with reversible and redundancy | NAT reversible/redundancy options are not included in the CC evaluated configuration. Therefore, updates to NAT reversible/redundancy are not applicable. |
| CSCwo47118 | Crash when clearing L2TP tunnels with the command clear vpdn tunnel l2tp | L2TP is not included in the CC evaluated configuration. Therefore, updates to L2TP are not applicable. |
| CSCwk79606 | PKI trustpoint password command only allows encryption type 0 and 7 | The fix corrects password obfuscation types. It has no direct impact to any TSF. |
| CSCwp02071 | Tunnels dropping when CAC configured for VDPN when CPU over threshold due to SSH request for SH tech | VPDN is not included in the CC evaluated configuration. Therefore, updates to VPDN are not applicable. |
| CSCwi59338 | Enable strict-kex support in IOS-SSH to address CVE-2023-48795 | This update adds optional SSH key exchange policy. The CC evaluated configuration already enforces approved algorithms. Therefore, the fix has no impact to TSF claims. |
| CSCwo00577 | Random crashes observed after tcp confg changes. | TCP tuning options are not included in the CC evaluated configuration. Therefore, updates to TCP config are not applicable. |
| CSCwn60286 | IOS-XE: Memory Leak observed in IPSEC/IKE session bringup with Cert-based Authentication | IPsec VPN is in scope, but this defect corrects internal memory handling during bringup. It does not change the TOE's implementation of IKEv2 or IPsec SFRs. Therefore, no impact to TSF claims. |
| CSCwn24226 | GETVPN Mismatch in GMs reported across COOP | GETVPN is not included in the CC evaluated configuration. Therefore, updates to GETVPN are not applicable. |
| CSCwn19586 | Certificate-based MACSEC flapping when dot1x reauth timers are set after reload | This defect affects stability during 802.1X reauth but does not alter CAK derivation, SAK lifecycle, or MACsec crypto enforcement. Therefore, no impact to TSF claims. |
| CSCwo89702 | Configuring logging discriminator name longer than 8 characters reloads standby switch. | The fix corrects a logging discriminator parser issue. It has no direct impact to any TSF. |
| CSCwn82786 | AAA settings not working based on template associated with the domain-name . | Template-based AAA configuration is not included in the CC evaluated configuration. Therefore, updates to AAA templates are not applicable. |
| CSCwn93483 | confd_cli high cpu utilization after executing show zbfw-dp sessions | ZBFW is not included in the CC evaluated configuration. Therefore, updates to ZBFW are not applicable. |
| CSCwm74060 | IOSD chasfs task crashes when retrieving platform info | The fix corrects platform info retrieval. It has no direct impact to any TSF. |
| CSCwm56800 | FIA trace packet decode displays incorrect value for fragmentation offset | The fix corrects diagnostic packet decoding. It has no direct impact to any TSF. |
| CSCwk78018 | Yang model does not handle properly default ikev2 authorisation policy | YANG modeling is not included in the CC evaluated configuration. Therefore, updates to YANG are not applicable. |
| CSCwm67178 | Cannot configure MD5 for the hash under the ikev2 proposal when compliance shield is disabled | MD5 is not an approved algorithm under the evaluated configuration. Therefore, this fix has no impact to TSF claims. |
| CSCwm48459 | Software crash with critical process vip_confd_startup_sh fault | The fix corrects an internal daemon crash. It has no direct impact to any TSF. |
| CSCwm89225 | CPP crashes After routing table changes | The fix corrects a data plane crash. It has no direct impact to any TSF. |
| CSCwk05354 | Interface flap with auto-neg CLI | Auto-negotiation features are not included in the CC evaluated configuration. Therefore, updates to auto-neg are not applicable. |

| Cisco Identifier | Title/Description | Rationale |
|---|---|---|
| CSCwm70520 | Device tracebacks generation | The fix corrects traceback logging. It has no direct impact to any TSF. |
| CSCwj33723 | Config not synced between active and third member of stack | Stack redundancy is not included in the CC evaluated configuration. Therefore, updates to stack sync are not applicable. |
| CSCwm50619 | Data policy commit failure occurs when export-spread is enabled in Cflowd configuration | Cflowd/NetFlow is not included in the CC evaluated configuration. Therefore, updates to Cflowd are not applicable. |
| CSCwn29062 | Traceback log output on device with data corruption error logs | Logging defect correction has no direct impact to any TSF. |
| CSCwm74317 | '%CRYPTO_ENGINE-4-CSDL_COMPLIANCE_RSA_WEAK_KEYS: RSA keypair CISCO_IDEVID_CMCA_SUDI | CSDL compliance enforcement is not included in the CC evaluated configuration. Therefore, updates to CSDL compliance are not applicable. |
| CSCwm54978 | Selinux: polaris_iosd_t denials | SELinux internals are not included in the CC evaluated configuration. Therefore, updates to SELinux are not applicable. |
| CSCwm77426 | Unexpected reload in NHRP, cache freed prior to function call | NHRP is not included in the CC evaluated configuration. Therefore, updates to NHRP are not applicable. |
| CSCwo72675 | All BFD sessions for dialer interfaces are down. SA ID is 0 for all of them. | BFD is not included in the CC evaluated configuration. Therefore, updates to BFD are not applicable. |
| CSCwp07901 | C8500 : CPP crash while processing fragments of a jumbo frame | The fix corrects jumbo frame handling in CPP. It has no direct impact to any TSF. |
| CSCwm27749 | Speed test download / Throughput issue on C8200 platform seen with IPSEC ESP-NULL transform using Zscaler | ESP-NULL/Zscaler overlays are not included in the CC evaluated configuration. Therefore, updates are not applicable. |
| CSCwo18836 | Transition Fugazi/C8500L from FBD to NSFBD | The fix corrects platform failover behavior. It has no direct impact to any TSF. |
| CSCwm58500 | MIP 100 stuck in booting state after ROMMON upgrade using 17.3(1r) rommon file. | The fix corrects a hardware module bootloader initialization issue. It has no direct impact to any TOE Security Function (TSF). It only ensures the MIP-100 card transitions correctly after a ROMMON upgrade. |
| CSCwm72748 | Crash in OMPd Process Crashes Due to Sig-abort When Hitting Pthread Limit. | The fix corrects an internal control-plane process stability issue. It has no direct impact to any TSF. It only ensures the OMPd daemon operates reliably under high thread counts. |