Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Maintenance Report for

Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18

Version 01.0, 22 April 2026

Document reference: AISEP-CC-MR-2026-AAC094

Table of contents

Introduction

Overview

This document is an Assurance Continuity Maintenance Report describing the findings of the Australian Information Security Evaluation Program (AISEP) concerning the certification of Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15.

The purpose of this Maintenance Report is to describe the status of the assurance continuity activities undertaken by Cisco Systems, Inc. against the requirements contained in Assurance Continuity: *CCRA Requirements v 3.1, 29 February 2024* (Ref [1]).

The Certification Report identifier for the evaluation and certification of Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15 is *AISEP-CC-CR-2025-EFT-T059-CR-V1.0* (Ref [5]).

Cisco Systems, Inc. submitted *Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18 Impact Analysis Report version 0.1* (Ref [2]) to the Australian Certification Authority (ACA) on 06 January 2026. The Impact Analysis Report (IAR) describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

Document / TOE Identification for the maintained TOE

- **IAR** - *Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18 Impact Analysis Report Version 1.0, 30 March 2026*
- **ST** - *Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18 Security Target, Version 2.1, 11 March 2026*
- **Guidance** – *Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18 Operational User Guidance and Preparative Procedures, Version 2.1, 11 March 2026*
- **Maintained TOE** - *Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18*

IAR introduction summary

The TOE is the Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18, developed by Cisco Systems, Inc.

The TOE is the Cisco Catalyst 8000V Edge (C8000V), a virtual router that functions as a virtual Network Device (vND) in accordance with the evaluated vND configuration described under Case 1 of the *NDcPP v3.0e Protection Profile (PP) [8]*. The TOE consists solely of the Cisco IOS-XE software, version 17.15, and running as a Virtual Machine (VM) on a hypervisor. The underlying hardware platform (Cisco UCS C-Series M7 server) and the ESXi 8.0 hypervisor are part of the Virtual System but are explicitly outside the TOE boundary. The TOE includes a virtual Route Processor and a virtual Forwarding Processor, both implemented in software within the VM.

Description of changes

The material in this section is a condensed version of the information in the *IAR* (Ref [2]).

TOE change outline

	Certified TOE (v17.15) →	Maintained TOE (v17.18)
Software/ Version	Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15	Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18
Hardware	None	None
Environment Change	None	None

Feature changes (summary)

The TOE is update from IOS-XE 17.15 to IOS-XE 17.18 introduces a set of new features and bug fixes that were reviewed and assessed by *Cisco Systems, Inc.* as non-security relevant with respect to the evaluated TOE. The enhancements primarily reflect ongoing product evolution, including improvements in deployment flexibility, platform and environment support, operational performance, and manageability. These feature updates are either operational in nature or fall outside the evaluated configuration defined in the *ST [3].*

All 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 by the *Cisco Systems, Inc.* and have no impact on the evaluated Security Functional Requirements, TOE Security Function interfaces, cryptographic services, or the TOE boundary. No new security-relevant functionality was introduced, and no changes were made to existing evaluated security functionality. Accordingly, the introduction of these features does not affect the previously certified TOE's security functionality claims.

CAVP Certificate Update Explanation

The underlying processor platform used in the evaluated configuration has **not changed** from the originally certified TOE.

The CAVP certificate number changed due to the integration of Cisco IC2M Rel5b in IOS-XE 17.18, replacing IC2M Rel5a used in IOS-XE 17.15.

The integration of IC2M Rel5b does not modify the implementation of any cryptographic algorithms claimed in the Common Criteria evaluation.

All cryptographic algorithms claimed in the evaluation remain implemented without change.

Affected developer evidence

	Certified TOE (v17.15) →	Maintained TOE (v17.18)
Security Target	Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15 Security Target, Version 1.0, 29 September 2025	Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18 Impact Analysis Report Version 0.1, 06 January 2026
Guidance Documentation	Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15, Operational User Guidance and Preparative Procedures, Version 1.0, Published 26 September 2025.	Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18 Operational User Guidance and Preparative Procedures, Version 2.1, 11 March 2026

Description of the developer evidence modifications

As part of the update from IOS-XE 17.15 to IOS-XE 17.18, limited modifications were made to the developer evidence to maintain alignment with the updated TOE. The *ST [3]* was updated to reflect the new IOS-XE 17.18 version identifier and associated configuration references. No changes were made to the evaluated Security Functional Requirements (SFRs), TOE Security Function (TSF) descriptions, security objectives, or assumptions, and the security claims remain unchanged from the certified baseline.

The *Operational User Guidance and Preparative Procedures (AGD) [4]* documentation was similarly updated to align with the IOS-XE 17.18 release. These updates were administrative and version-specific in nature, ensuring consistency with the updated TOE identification and supported deployment environments. No changes were introduced that affect evaluated functionality, secure configuration requirements, or operational guidance relevant to the Common Criteria evaluation.

Regression testing

IOS-XE 17.18 was developed under Cisco's controlled software development lifecycle. All defect corrections included in this update were subject to targeted functional verification to confirm that the identified issue was resolved and that no unintended side effects were introduced.

In addition to defect-specific verification, predefined regression test suites were executed to confirm that previously implemented functionality continued to operate as specified following the update from IOS-XE 17.15 to IOS-XE 17.18 as a minor change under Assurance Continuity.

Regression validation activities included:

- Functional confirmation of corrected defects
- Stability verification of affected subsystems
- Confirmation that no changes were made to evaluated Security Functional Requirements (SFRs)
- Verification that no new TSF interfaces were introduced
- Confirmation that cryptographic services and interfaces remained unchanged

The Cisco's regression analysis determined that:

- No modifications were made to any evaluated SFR implementation
- No changes were made to TOE interfaces relevant to the evaluation
- No changes were made to the cryptographic boundary

Therefore, the results of regression validation demonstrate that the evaluated security functionality continues to operate as defined in the certified baseline.

Vulnerability analysis

A vulnerability review was conducted on January 6, 2026 by Cisco Systems, Inc. in support of this Assurance Continuity submission to determine whether IOS-XE 17.18.1 introduces any new vulnerabilities affecting the evaluated configuration.

The review included publicly available vulnerability sources:

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.cve.org/
- https://nvd.nist.gov/vuln/search

In addition, the review included:

- Cisco Product Security Incident Response Team (PSIRT) advisories
- Internal defect tracking for security-relevant issues

The following product identifiers and related terms were used as search criteria:

- Cisco Catalyst 8000V Edge
- C8000V

- Cisco IOS-XE 17.18 / 17.18.1a
- Intel Xeon Platinum 8452Y (Sapphire Rapids)
- IC2M Rel5b
- CiscoSSL
- CiscoSSH

The review confirmed that:

- All publicly disclosed vulnerabilities applicable to the evaluated configuration have been addressed in IOS-XE 17.18.1a
- No new exploitable conditions affecting the evaluated Security Functional Requirements were introduced
- No changes were made to TSF interfaces or cryptographic services

Accordingly, the vulnerability posture of the TOE remains consistent with the certified baseline.

Conclusion

After consideration of the *Impact Analysis Report* (Ref [2]) provided by Cisco Systems, Inc. the Australian Certification Authority (ACA) has determined that the described changes are **minor**. The ACA agrees that the resultant change in the TOE can be classified as minor and that certificate maintenance is the correct path to continuity of assurance. The ACA agrees that the original assurance result is acceptable for the maintained TOE, Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18.

Annex – References and Abbreviations

References

1. *Assurance Continuity: CCRA Requirements, version 3.1. 29 February 2024.*
2. *Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18 Impact Analysis Report Version 1.0, 30 March 2026.*
3. *Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18 Security Target, Version 2.1, 11 March 2026.*
4. *Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.18 Operational User Guidance and Preparative Procedures, Version 2.1, 11 March 2026*
5. *Certification Report Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15 Version 1.0, 28 October 2025 Report Identifier: AISEP-CC-CR-2025-EFT-T059-CR-v1.0.*
6. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
7. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
8. *collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023*

Abbreviations

ACA	Australian Certification Authority
AISEP	Australian Information Security Evaluation Program
CCRA	Common Criteria Recognition Arrangement
IAR	Impact Analysis Report
SFR	Security Functional Requirement
ST	Security Target
TSFI	TOE Security Function Interface
TOE	Target of Evaluation

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)