CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Cisco 1000 Series Integrated Services Routers (C1100), Cisco Catalyst IR1800 Rugged Series Routers (IR1800), Cisco Catalyst IR8300 Rugged Series Routers (IR8300) running IOS-XE 17.18

Maintenance Report Number: CCEVS-VR-VID11643-2026

Date of Activity: May 15, 2026

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." 29 August 2014.

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

Cisco 1000 Series Integrated Services Routers (C1100), Cisco Catalyst IR1800 Rugged Series Routers (IR1800), Cisco Catalyst IR8300 Rugged Series Routers (IR8300) running IOS-XE 17.18 Security Target Version: 2.0 October 23, 2025

Cisco 1000 Series Integrated Services Routers (C1100), Cisco Catalyst IR1800 Rugged Series Routers (IR1800), Cisco Catalyst IR8300 Rugged Series Routers (IR8300) running IOS-XE 17.15 Operational User Guidance and Preparative Procedures, Version 1.0 October 7, 2025

Cisco 1000 Series Integrated Services Routers (C1100), Cisco Catalyst IR1800 Rugged Series Routers (IR1800), Cisco Catalyst IR8300 Rugged Series Routers (IR8300) running IOS-XE 17.18 Impact Analysis Report Update IOS-XE 17.15 to 17.18 Version: 0.1 December 17, 2025

collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 (CPP_ND_V3.0E)

PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 16 August 2023 (MOD_VPNGW_1.3)

Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021 (PKG_SSH_V1.0)

PP-Configuration for Network Devices and VPN Gateways, Version 2.0, 25 April 2024 (CFG_NDcPP-VPNGW_V2.0)

Affected Developer Evidence:

Cisco 1000 Series Integrated Services Routers (C1100), Cisco Catalyst IR1800 Rugged Series Routers (IR1800), Cisco Catalyst IR8300 Rugged Series Routers (IR8300) running IOS-XE 17.15 Security Target, Version 1.0 October 7, 2025

Cisco 1000 Series Integrated Services Routers (C1100), Cisco Catalyst IR1800 Rugged Series Routers (IR1800), Cisco Catalyst IR8300 Rugged Series Routers (IR8300) running IOS-XE 17.15 Operational User Guidance and Preparative Procedures, Version 1.0 October 7, 2025

Updated Developer Evidence:

This assurance maintenance request is to update IOS-XE from version 17.15 to version 17.18, to incorporate a number of new features (26) and bug fixes (22), and update the CAVP Certificate from A1462 to A4354. The developer has provided sufficient supporting rationale describing the impact of each change. Both the Security Target and the Guidance Document were updated to identify the new IOS-XE version. The Security Target references the updated CAVP A4354.

Description of ASE Changes:

An Impact Analysis Report (IAR #1) was submitted to CCEVS for Cisco to update IOS-XE from version 17.15 to version 17.18, to incorporate a number of new features (26) and bug fixes (22), and update the CAVP Certificate from A1462 to A4354.

The New Features (26) described in the IAR cover a range of areas; none of which are identified as security relevant. Cellular connectivity enhancements account for 10 of these, and thirteen (13) others cover basic networking and hardware enhancements, e.g., power-failure notification feature, resource allocation, and support for WiFi6. The remaining three (3) do cover features generally considered security relevant, i.e., MACsec support, Web Authentication support, and 802.1x authentication. However, since these are outside the scope of the evaluated functionality for this Security Target, they are also considered not security relevant.

The Bug Fixes (22) described in the IAR cover a range of areas; 20 of which cover areas not security relevant and have no direct impact on any TOE Security Function. These include configuration of the cellular controller, cellular MTU interface issues, system stability, memory leaks, and SNMP. Two of the bug fixes do address areas covered by SFRs. The first addresses an NTP synchronization issue directly supporting the reliable time stamp security function (FPT_STM_EXT.1, FCS_NTP_EXT.1). It ensures the accuracy of security-relevant timestamps. The second fix addresses a firmware upgrade failure, which is part of maintaining the system's integrity and trusted update mechanism (FPT_TUD_EXT.1). It ensures the expected functionality of updates. The IAR states in the summary section that no bug fixes are security relevant.

Although the CAVP has been updated from CAVP A1462 to CAVP A4354 in the assurance maintenance release, the core processors remain the same, Marvell Armada (Cortex-A72) and Intel Atom C3708 (Goldmont). The CAVP tables in the validated ST and the updated ST in the assurance maintenance request, are identical except for the reference to the CAVPs, CAVP A1462 to CAVP A4354, respectively. The IAR hints at, but do not actually reference, the CMVP certificate numbers. CMVP Cert number 4752 shows CAVP A4352 for the updated ST, and CMVP Cert number 4222 shows CAVP A1462 for validated ST. Therefore the CAVP Certificates remain valid.

Changes to TOE:

The only changes to the TOE were the update of IOS-XE from version 17.15 to version 17.18, to incorporation of a number of new features (26) and bug fixes (22), and update the CAVP Certificate from A1462 to A4354. The software changes had no impact on the evaluated configuration. Those software changes that did, had only minor impact.

Description of ALC Changes:

1. Security Target – The Security Target has been updated to note the update of IOS-XE from version 17.15 to version 17.18. No other changes were necessary to the Security Target as all changes were minor and did not impact the ST.
2. Guidance document – The Guidance document was updated to note the update of IOS-XE from version 17.15 to version 17.18. No other changes were necessary.

Assurance Continuity Maintenance Report:

- An Impact Analysis Report (V1.0) was submitted to update of IOS-XE from version 17.15 to version 17.18, add a number of new features, a number of software bug fixes, and to update the CAVP from A1462 to A4354.
- There are no security relevant fixes so no new evaluation is required.
- No development environment changes occurred that impacted the product.
- There were no changes that required the evaluators to do any additional testing.

Description of Regression Testing:

During development of the 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..

Vulnerability Assessment:

A search of the following national sites was conducted on May 22, 2026:

https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://www.cve.org/
https://nvd.nist.gov/vuln/search#/nvd/home?resultType=records

The following key words, product, and vendor were each selected as search criteria for vulnerabilities related to the TOE:

- Cisco 1000 Series Integrated Services Routers
- Cisco Catalyst IR1800 Rugged Series Routers
- Cisco Catalyst IR8300 Rugged Series Routers
- Cisco C1101 Integrated Services Routers
- Cisco C1109 Integrated Services Routers
- Cisco C1111 Integrated Services Routers
- Cisco C1112 Integrated Services Routers

- Cisco C1113 Integrated Services Routers
- Cisco C1116 Integrated Services Routers
- Cisco C1117 Integrated Services Routers
- Cisco C1118 Integrated Services Routers
- Cisco C1121 Integrated Services Routers
- Cisco C1126 Integrated Services Routers
- Cisco C1127 Integrated Services Routers
- Cisco C1128 Integrated Services Routers
- Cisco C1131 Integrated Services Routers
- Cisco C1161 Integrated Services Routers
- Cisco C1101 Integrated Services Routers
- Cisco Catalyst IR1835-K9
- Cisco Catalyst IR1821-K9
- Cisco Catalyst IR1831-K9
- Cisco Catalyst IR1833-K9
- Cisco Catalyst IR1840-K9
- Cisco Catalyst IR8340-K9
- ARM Cortex-A72
- Intel Atom C3708
- IC2M Rel5b
- Cisco IOS-XE 17.18
- CiscoSSL
- CiscoSSH

Appendix A, Table 6 are the vulnerabilities found as of May 22, 2026, and how they were addressed by Cisco. All the vulnerabilities listed have been addressed in the IOS-XE 17.18.1a release (version of the TOE under Assurance Maintenance).

The IAR contains the output from the vulnerability searches and the rationale why the search results are not applicable to the TOE. This search was performed on May 22, 2026. No vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

The changes are divided into an IOS-XE update, new features, and bug fixes. The subsections above justify that these changes have no security relevance on the certified TOE.

Validation Team Conclusion:

The validation team reviewed the changes and concurred the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The Security Target and the Guidance Document were updated to specify the new version of the IOS-XE 17.18.1a.

Based on this and other information from within this IAR document, the Validation Team agrees that the assurance impact of these changes is minor.