



ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco Embedded Services Router (ESR) 6300 running IOS-XE 17.18

Maintenance Update of Cisco Embedded Services Router (ESR) 6300 running IOS-XE 17.18

Maintenance Report Number: CCEVS-VR-VID11582-2026

Date of Activity: 16 July 2026

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016.
- Cisco Embedded Services Router (ESR) 6300 running IOS-XE 17.18 Impact Analysis Report, Version 0.3, July 7, 2026,

Evaluated TOE

- **VR Title:** Cisco Systems, Inc. Embedded Services Router (ESR) 6300 V17.15
- **VR Report #:** CCEVS-VR-VID11582-2025
- **VR Version** – 1.0
- **VR Date** –July 18, 2025

Current AM TOE Updated

- **ACMR Title** – ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco Embedded Services Router (ESR) 6300 running IOS-XE 17.18
- **ACMR Report #:** CCEVS-VR-VID11582-2026
- **ACMR Version** – 1.0
- **ACMR Date** – July 16, 2026

Documentation Updated:

CC Evidence	New Evidence Change	Change Summary
Cisco Embedded Services Router (ESR) 6300 v17.15 Security Target Version 1.0, July 14, 2025	Cisco Embedded Services Router (ESR) 6300 v17.18 Common Criteria Security Target Version 2.2, July 7, 2026	Updated to reflect IOS-XE version 17.18 software version number. Document Title change.

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

Cisco Embedded Services Router (ESR) 6300 v17.15 Operational User Guidance and Preparative Procedures, Version 1.0, July 14, 2025	Cisco Embedded Services Router (ESR) 6300 v17.18 Common Criteria Configuration Guide, Version 2.0, October 10, 2025	The CC Configuration Guide was updated to IOS-XE version 17.18. Document Title change.
---	---	--

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 last updated IAR was submitted on 16 July 2026. 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:

No new features have been introduced into the ESR 6300 since the certification of the IOS-XE 17.15 version.

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

Cisco Identifier	Title/Description	Rationale
CSCwk45528	ESR6300 enters to ROMMON with any key	Only users with physical access to the device (console access) can encounter this bug, so defense in depth is what protects the device. It's assumed that the device is protected from being physically accessed by unauthorized users.
CSCwo24897	ESR6300 with SLR does not install 2G or uncapped license after reload.	The fix corrects a license process fault. It has no direct impact to any TSF.
CSCwn52402	In the platform, ESR-6300-NCP-K9, we may lose the configuration after removing the SLA trustpoint.	This fix corrects an internal platform process issue and has no direct impact to any TSF.

These changes have been assessed as minor. These enhancements do not affect the security functionality or claims of the previously evaluated TOE.

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 the new IOS-XE version, there were various tests performed to ensure the product performs as expected. Bug fixes were 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.

NIST Certificates:

The implementation of the validated cryptographic algorithms has not been modified upon integration into the TOE, as the Cisco IC2M Rel5a and Rel5b are used in the IOS-XE 17.15 and 17.18 versions, respectively. All cryptographic algorithms claimed in the Common Criteria evaluation (AES-CBC, AES-GCM, SHA family, HMAC, RSA, ECDSA, approved key agreement schemes, and CTR_DRBG) are retained in Rel5b without change. Rel5b removes certain legacy algorithms (e.g., 3DES, older TLS PRFs) that were present in Rel5a but not claimed in the evaluation; this deprecation has no effect on the evaluated security posture. It also adds new algorithms (SHA-3, TLS 1.3 KDF), but none of the new algorithms are claimed by the TOE. Therefore, the cryptographic algorithm implementation validated for CAVP conformance also applies to the changed TOE, and the evaluated Security Functional Requirements remain satisfied, supporting the Assurance Maintenance justification.

Vulnerability Assessment:

A search of the following national sites was conducted on July 7, 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 Embedded Services Router ESR 6300
- ESR 6300
- Marvel Armada 88F7040
- Cisco IOS-XE 17.18
- IC2M Rel5b
- CiscoSSL
- CiscoSSH

All the vulnerabilities listed have been addressed in the IOS-XE 17.18.1a release version of the TOE under Assurance Maintenance.

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

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

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.