ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco Catalyst 3650 and 3850 Series Switches

Maintenance Update of Cisco Catalyst 3650 and 3850 Series Switches

Maintenance Report Number: CCEVS-VR-VID10940-2019

Date of Activity: 17 December 2019

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016;
- Cisco Catalyst 3650 and 3850 Series Switches Impact Analysis Report for Common Criteria Assurance Maintenance, version 1.0, 4 December 2019
- collaborative Protection Profile for Network Devices + Errata 20180314, Version 2.0e; and
- Network Device Collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption (MACsec EP), version 1.2

Documentation reported as being updated:

- Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.12 Common Criteria Security Target, Version 2.0, 4 December 2019; and
- Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.12 Common Criteria Operational User Guidance And Preparative Procedures, Version 2.0, 4 December 2019

Assurance Continuity Maintenance Report:

Cisco Systems, Inc., submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 4 December 2019. 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 3.0. 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, IAR, and User Guidance. The Security Target was revised to update the IOS-XE software and ST version numbers. The User Guide was also revised to update the IOS-XE software and Guide version numbers.

The IAR was new and identifies the changes to the TOE included correcting functional issues and making related changes to various documents.

Changes to TOE:

Software bug fixes resulted in what were considered "Minor Changes". Such changes were described as non-security relevant, functional, and having no direct impact to any TOE Security Function.

Eleven such changes were listed in the IAR along with a description and given rationale. The description and rational for each were inspected and the overall Minor Change characterization was considered appropriate. None of the changes resulted in the introduction of new TOE capabilities, changes to the TOE boundary, or were numerous enough to have major impact. Changes related to the handling of end host traffic; memory leaks; queue maintenance; Dynamic Host Configuration Protocol (DHCP) handling; interface management and accessibility; switch crashes, and DB cursor handling. All changes only ensured that the products function as expected.

There were no Major Changes.

In addition, there were no changes made in the processor used and the bug fixes to the OS version had no effect on cryptographic processing. Therefore, no modifications were required in any of the existing NIST certificates.

Regression Testing:

Although no changes were directly made to the security functionality, the IAR reported that "Each individual change was unit tested, and the IOS-XE 16.12 software image has had a limited amount of automated regression testing covering all major areas of baseline client functionality."

Vulnerability Analysis:

The vendor conducted searches of public vulnerability sites and, using selected key words and product identifiers, located a group of published vulnerabilities. All were reviewed and were either identified as having no impact on the TOE or were listed as having been addressed in the TOE version presented as part of this Assurance Maintenance Action.

Conclusion:

CCEVS reviewed the description of the changes and found them all minor. All bug fixes were for non-security relevant functions and did not affect any TOE Security Functions. Regression testing was done and was considered adequate based on the scale and types of changes made.

The vendor also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance.

In addition, the hardware models did not change and there were no necessary alterations to the NIST cryptographic certificates.

Therefore, CCEVS agrees that the original assurance is maintained for the product.