ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco Email Security Appliance

---

Maintenance Update of Cisco Email Security Appliance

Maintenance Report Number: CCEVS-VR-VID10798-2017a

Date of Activity: 20 October 2017

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- Cisco Email Security Impact Analysis Report For Common Criteria Assurance Maintenance, Version 0.1, September 13, 2017
- collaborative Protection Profile for Network Devices, Version 1.0, 27-Feb-2015

Documentation reported as being updated:

- Cisco Email Security Appliance Security Target, Version 1.0, 13 September 2017;
- Cisco Email Security Appliance CC Configuration Guide, Version 1.0, 14 September 2107

Assurance Continuity Maintenance Report:

Cisco Systems, Inc., submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 17 October 2017. 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 IAR identifies the changes to the TOE included adding a new hardware component, clarifying changes in model version identification, and making related changes to various documents.

The evaluation evidence consists of the Security Target, Impact Analysis Report (IAR), and User Guidance. The Security Target was revised to introduce a new piece of supported hardware and clarify pieces of supported hardware whose references in the evaluated version of the ST were incorrect. The User Guide was revised to identify those same corrected hardware components. The IAR was new.

The evaluation was done against the collaborative Protection Profile for Network Devices and the ST referenced validated FIPS certificates. No changes were made in the processor, and the bug fixes to the OS version had no effect on cryptographic processing, so no modifications were required in any of the valid NIST certificates.

Changes to TOE:

Software bug fixes were made to non-security relevant system functions. Also, the listings, in the ST and guide document, of originally incorrect hardware models were corrected but that had no effect on the TOE itself. A list of the various bug fixes was presented in the IAR and all were listed as being either associated with non-security relevant commands and configuration or for functions/components not claimed in the original evaluation (e.g., Cisco Advanced Malware Protection, antivirus functions, clustering, content filtering, etc.). Rational was included for why the various bug fixes did not affect the TOE.

Changes to Evaluation Documents:

- ST: Updated to add the C690X model and update the list of TOE Hardware Models listed in ST Table 3 to correct typographical errors.
- AGD_PRE and OPE: Updated to add new hardware model and to correct typographical errors in the list of supported hardware and to reflect updated software versions

  All these changes were made to either correct errors in the original evaluated versions of the ST and CC configuration guide document or to add a new hardware version.

Regression Testing:

Although no changes were made to the security functionality of the TOE, but a new hardware model was added, and testing was rerun. The same Test Plan used for the original evaluation was used. New test results were generated, and were reviewed by Cisco. An updated search for vulnerabilities was also done for the updated TOE version. No new vulnerabilities were detected.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found them all to be minor. The inclusion of the C690X Hardware Model does not change any of the security functions that are claimed in the Security Target. All the security functions claimed are enforced by the Cisco Email Security Appliance software and not the hardware components.

All bug fixes were for non security-relevant functions and did not affect any TOE Security Functions.

The hardware model added was to an existing series of supported models. Those modules only served a functional role in the original evaluation so no security testing directly examined them. The vendor reported, however, that the new modules did undergo regression testing.

The CCTL also reported that there were no vulnerabilities associated with any of the models.

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