ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
Cisco Email Security Appliance

Maintenance Update of Cisco Web Security Appliance

Maintenance Report Number: CCEVS-VR-VID10799-2018

Date of Activity: 30 January 2018

References:

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

Documentation reported as being updated:

- Cisco Web Security Appliance Security Target, Version 1.1, August 2017;

Assurance Continuity Maintenance Report:

Cisco Systems, Inc., submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 27 December 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 Assurance Continuity action was made in order to demonstrate compliance with NIAP Labgram #106.

The IAR identifies that four additional ciphersuites were added to the ST, but that no changes were otherwise made to the TOE hardware or software. Those ciphersuites were tested in the original evaluation but were not included as selections in the associated SFR (i.e.., FCS_TLSS_EXT.1.1).

The evaluation evidence consists of the Security Target and the Impact Analysis Report (IAR). The Security Target was revised to reflect the full set of TLS ciphersuites supported and to be compliant with Labgram #106. The IAR was new.

The evaluation was done against the collaborative Protection Profile for Network Devices Version 1.0 and the ST referenced validated FIPS certificates. No changes were made in the processor and no modifications were required in any of the valid NIST certificates.

Changes to TOE:

None.

Changes to Evaluation Documents:

- ST: Updated FCS_TLSS_EXT.1.1 to add the following ciphersuites:
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289

Regression Testing:

Testing was completed with TLS prior to the product being certified in August 2017. That testing included the four TLS ciphersuites that have been added to the ST. However, additional tests of the four additional ciphersuites was performed with the evaluated version of the TOE, and demonstrated to work correctly with no observable consequences. That additional testing was performed as part of this Assurance Continuity activity.

Vulnerability Analysis:

No additional vulnerability analysis was performed since there were no changes made to the TOE, either in hardware or software.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found them all to be minor. All the security functions claimed are enforced by the Cisco Web Security Appliance.

The ST was updated to reflect the full set of TLS ciphersuites supported by the Cisco Web Security Appliance. The evaluation is now considered to be compliant with NIAP Labgram #106.

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