ASSURANCE CONTINUITY MAINTENANCE REPORT FOR AhnLab MDS, MDS with MTA, and MDS Manager V2.1

Maintenance Update of AhnLab MDS, MDS with MTA, and MDS Manager V2.1

Maintenance Report Number: CCEVS-VR-VID10818-2019

Date of Activity: 16 January 2019

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Impact Analysis Report Version 1.9, July 9, 2018
- collaborative Protection Profile for Network Devices, Version 1.0, February-2015

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Security Target, Version 0.7, July 7, 2018	**Maintained Security Target:** AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Security Target, Version 0.92, December 20, 2018 Changes in the maintained ST are: • Updated identification of ST • Updated device software version • Updated the Operating System version • Added appliance models • Updated documentation references • Updated OpenSSL version • Updated OpenSSH version
Common Criteria Compliance Guide: MDS V2.1, MDS Manager V2.1, MDS	**Maintained Common Criteria Compliance Guide:** MDS V2.1, MDS Manager V2.1, MDS (MTA

(MTA License Applied) V2.1, Configuring Common Criteria Compliance Guide, Document version: v0.4 (2018.02.09)	License Applied) V2.1, Configuring Common Criteria Compliance Guide, Document version: v0.4 (2018.11.19) Changes in the maintained Guidance are: • Updated the list of TOE Hardware Models to include the MDS 4000A MDS 4000A, MDS 8000A, MDS10000A, MDS with MTA 4000a, MDS with MTA 8000A, MDS with MTA models.
Test: AhnLab MDS, MDS with MTA, and MDS Manager V2.1 IAR Testing, Version 1.0, March 5, 2018	**Maintained Test Report** AhnLab MDS 4000A, 8000A, and 10000A IAR Testing Report Version 1.0, December 21, 2018

Assurance Continuity Maintenance Report:

AhnLab, Inc., submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 27 December 2018. 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, the CC Compliance Guide, Test Report and the Impact Analysis Report (IAR). The ST and guide document were updated, IAR and the test evidence were new.

The evaluation was done against the collaborative Protection Profile for Network Devices Version 2.0 and the ST referenced validated CAVP certificates. No changes were made in the processor and no modifications were required in any of the valid NIST certificates.

Changes to TOE:

For this Assurance Continuity, the following TOE software version updates were released:

- The TOE MDS Analyzer software was updated from version 2.1.8.27 to version 2.1.8.29 due to the update of the third-party OpenSSL;
- The Data Viewer software was updated from version 2.1.8.30 to version 2.1.8.31 due to the update to the third-party OpenSSL and the update to OpenSSH;
- The Linux kernel update from version 4.16.4 to version 4.18.16;
- The DB Pgsql (Postgress) update from 9.6.6 to PostgreSQL 11.1; and
- The addition of three new hardware models: MDS 4000A, MDS 8000A, and MDS 10000A.

The updates to AhnLab MDS, MDS with MTA, and MDS Manager V2.1 were the result of

mitigating the third-party vulnerabilities and the addition of hardware specifications for two new TOE appliances.

No functionality, as defined in the SFRs, was impacted, and none of the software updates or the addition of the three MDA devices affected the security functionality or the SFRs identified in the Security Target. All updates are, therefore, considered to be Minor Changes.

Changes to Evaluation Documents:

- ST: modified to reflect changes to TOE software that were required by an update to a third-party OpenSSL/OpenSSH modules and to add a number of new supported hardware models; and
- Common Criteria Compliance Guide: modified to reflect the new set of supported hardware models.

Regression Testing:

Regression testing was performed on the three new MDS devices with the MDS Analyzer 2.1.8.29 and the Data Viewer 2.1.2.31. The test cases verified that the three new MDS devices generated the correct results and did not affect the security functionality defined in the Security Target. The functionality of the additional MDS 4000A, MDS 8000A, and MDS 10000A models remains the same as prior MDS models. The additional models differ in the main processor, storage, and network ports. The size of storage and the number of network ports has no effect on the security functionality of the product. The same version of the Data Viewer software was implemented on all TOE devices including the MDS, MDS with MTA, and the MDS Manager. Since testing verified the correct operation on the MDS device, the same software will produce equivalent results on all of the TOE devices.

NIST CAVP Certificates:

The CAVP certificates for the AhnLab MDS ACM, Version 1.0 cryptographic module were verified to be current and active.

CAVP testing was performed against the Intel Xeon processors. The MDS 4000A devices contain an Intel Xeon ten Core processor, the MDS 8000A devices contain a ten-core processor, and the MDS 10000A contain an Intel Xeon twenty core processor. Therefore, all the devices are covered by the same CAVP certificates as defined in the Security Target.

The TOE includes the AhnLab MDS OpenSSL cryptographic module: AhnLab MDS ACM, Version 1.0. The module comprises a vendor-modified version of the OpenSSL FIPS Object Module 2.0.12 linked with the FIPS-capable OpenSSL 1.0.2p and OpenSSH 7.8p1 libraries. The AhnLab MDS ACM v1.0 (Firmware) was not affected by the third-party software updates, including the update to Linux kernel 4.18.16. The TOE updates of the OpenSSL 1.0.2p and OpenSSH 7.8p1 did not affect the CAVP certifications since the AhnLab Cryptographic Module (ACM) binary has not been modified.

Vulnerability Analysis:

The evaluation team searched the public domain for any new vulnerabilities that may have been identified since the last Maintenance Assurance was completed. Mitigation rationale was provided for all new vulnerabilities for third-party software that did not include a software update. The software updates were the result of third-party vulnerabilities. The vulnerability fixes did not change the functionality of any of the third-party products, only corrected for vulnerabilities. The third-party software updates to PostgreSQL 11.1, and OpenSSL 1.0.2.p/OpenSSH 7.8p1, mitigated the vulnerabilities and the TOE is no longer vulnerable.

The upgrade from Linux Kernel 4.16.4 to 4.18.16 was due to recognized Linux vulnerabilities that did not impact the TOE. The upgrade was the latest version available and had no further impact on the TOE.

Since none of the updates changed the functionality and the testing produced the correct results, the overall update to the TOE can be considered Minor.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor.

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