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 with software patch 2.1.8.26

Maintenance Report Number: CCEVS-VR-VID10818-2017a

Date of Activity: 30 June 2017

References: Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004;

Impact Analysis Report (IAR) for AhnLab MDS, MDS with MTA, and MDS Manager V2.1, Version 1.0, 14 June 2017

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 0.3, April 26, 2017	**Maintained Security Target:** AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Security Target, Version 0.4, June 14, 2017 Changes in the maintained ST are: • Updated identification of ST • Updated device software version • Added appliance models.
Common Criteria Compliance Guide: MDS V2.1, MDS Manager V2.1, MDS (MTA License Applied) V2.1, Configuring Common Criteria Compliance Guide, Document version: v0.2 (2016.06.27)	**Maintained Common Criteria Compliance Guide:** MDS V2.1, MDS Manager V2.1, MDS (MTA License Applied) V2.1, Configuring Common Criteria Compliance Guide, Document version: v0.3 (2017.05.17)

	Changes in the maintained Guidance are: • Updated the list of TOE Hardware Models to include the MDS 4000, MDS 4000 with MTA, MDS 8000, and MDS 8000 with MTA models.
Test: AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Test Report and Procedures, Version 1.2, April 12, 2017	**Additional Models Test:** AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Additional Device Sampling Test Report, Version 1.0, June 12, 2017

Assurance Continuity Maintenance Report:

The vendor for the AhnLab MDS, MDS with MTA, and MDS Manager V2.1 submitted an IAR to CCEVS for approval on 14 June 2017. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. 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 changes described in this document constitute all changes made to the AhnLab MDS, MDS with MTA, and MDS Manager V2.1 since the previous Common Criteria evaluation, CCEVS-VR-VID10818-2017.

Changes to TOE:

The AhnLab MDS, MDS with MTA, and MDS Manager V2.1 updates were the result of the addition of four new hardware models. Minor firmware upgrades were made to support the new models and mitigate newly found vulnerabilities in PostgreSQL (pgsql) 9.6.2. The TOE was upgraded to PostgreSQL (pgsql) 9.6.3. This resulted in a minor TOE version changes:

- MDS Analyzer 2.1.8.25 -> 2.1.8.26
- Data Viewer 2.1.8.25 -> 2.1.8.26

New Appliance Models

Device	Main Processor	Storage	Network Ports	Operating System
MDS 4000	Intel Xeon 10 Core	HDD: 2TB, SSD: 480GB	1GbE (Copper) 4ea	Linux 3.14.18
MDS 4000 with MTA	Intel Xeon 10 Core	HDD: 2TB, SSD: 480GB	1GbE (Copper) 4ea	Linux 3.14.18
MDS 8000	Intel Xeon 12 Core 2ea	HDD: 4TB, SSD: 1.2GB	1GbE (Copper) 4ea	Linux 3.14.18
MDS 8000 with MTA	Intel Xeon 12 Core 2ea	HDD: 4TB, SSD: 1.2GB	1GbE (Copper) 4ea	Linux 3.14.18

The specific changes made to the firmware minor version and the addition of two MDS and two MDS with MTA devices do not affect the security claims in the AhnLab MDS, MDS with MTA, and MDS Manager V2.1 Security Target.

Regression Testing

Regression testing was performed on the added MDS appliance devices. The MDS with MTA appliances were not tested because the two device models are considered equivalent platforms. The MDS and MDS with MTA devices have the same software installed. Test cases sampled and described in the updated test evidence were validated with the current (revised) version of the firmware. Test results were produced and found consistent with the previous test results.

Cert Analysis

The new models use the same Intel Xeon processor and Linux 3.14.18 OS as the models tested under the CCEVS-VR-VID10818-2017 evaluation. Thus, no new CAVP certs are required.

Vulnerability Analysis

A public search for new vulnerabilities that might affect the TOE since the evaluation was performed. In summary, no vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via the firmware minor version update.

The vulnerabilities that were identified are for the third-party product DB Pgsql(Postgress) 9.6.2 which is used by the TOE. AhnLab mitigated the vulnerability by updating the TOE to use DB Pgsql(Postgress) 9.6.3. No vulnerabilities were identified in DB Pgsql(Postgress) 9.6.3. The firmware update resulted in a firmware minor version update.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found it to be minor. Therefore, CCEVS agrees that the original assurance is maintained for the above-cited version of the product.

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT