ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Samsung SDS EMM v1.5.1 with Patch for iOS11

Maintenance Update of Samsung SDS EMM v1.5.1 with Patch for iOS11

Maintenance Report Number: CCEVS-VR-VID10751-2018

Date of Activity: 31 August 2018

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016;
- Impact Analysis Report for Samsung SDS EMM v1.5.1 with Patch for iOS11, Revision 1.0, July 4, 2018
- Protection Profile for Mobile Device Management, Version 2.0, December 31, 2014
- Extended Package for Mobile Device Management Agents, Version 2.0, December 31, 2014

Documentation reported as being updated:

- Samsung SDS Co., LTD EMM (MDMPP20/MDMAEP20) Security Target, Version 0.4, 2016/12/22
- Samsung SDS EMM Administrator's Guide, Version 1.5.1, December 2016
- Samsung SDS EMM Installation Guide, Version 1.5.1, December 2016
- Samsung SDS Push Installation Guide, Version 1.5.1, December 2016
- Samsung SDS AppTunnel Installation Guide, Version 1.5.1, December 2016

Assurance Continuity Maintenance Report:

The Samsung SDS EMM TOE is an Enterprise Mobility Management product designed to provide centralized management of mobile devices and associated applications. The TOE comprises a server component, which allows an organization to define device management policies, and an Agent component, which enforces the device management policies on each device. There are separate Agents for Android devices and iOS devices.

Samsung SDS Co., Ltd, submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval in July 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 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.

Changes to TOE:

Changes to the TOE included updates to the TOE's server component to address modifications in behavior on iOS devices, and changes to the TOE's client components for Android to address changes to Knox containers. The Android component has also been updated and operates on several new evaluated phone platforms.

The server component was patched to accommodate a change in the SCEP behavior that was implemented in iOS devices regarding the handling of special characters. The updated server software now handles blanks in Base64 encoded strings in Certificate Signing Requests (CSRs) with '+' and other URL encoding and decoding changes. The server component also now uses the replaced API for the EMM Client activation API specification that was changed in iOS11. These changes are all minor and are not deemed to have any security relevance.

The client component for Android was patched to accommodate modifications to the Knox container's numbering scheme, which changed the user ID's initial value of 100 to an initial value of 10 in line with changes introduced beginning in Android 8. The client has implemented a mapping function to ensure that all versions are treated appropriately. The changes to the numbering scheme and the addition of a mapping function are minor and did not warrant any changes to execute successfully on the newly added devices.

The Android client component was also updated and tested to verify that it works on the following currently evaluated phone platforms[1]:

- (NIAP VID 10898) Samsung Galaxy Devices on Android 8: Samsung Galaxy S8, S8+, S8 Active, Note 8, S9 and S9+.
- (NIAP VID 10849) Samsung Galaxy Devices on Android 7.1: Samsung Galaxy Note8 and Tab Active 2.
- (NIAP VID 10809) Samsung Galaxy Devices with Android 7: Samsung Galaxy S6, S6 Active, S6 Edge, S6 Edge+, Note 5, S7, S7 Active, S7 Edge, S8, S8 Active, S8+, and Tab S3.

These platforms all have a common device management Application Programming Interface (API) and operate in a virtual environment that abstracts the applications from the hardware. Additionally, although the new devices execute on several new versions of the Android operating system, the underlying cryptographic capabilities provided by these operating systems have been

[1] Note that some device models (e.g. the Samsung Galaxy Note 4, S6, and S7 on Android 6.0.1) and related prior evaluations (e.g. VID10725) have been removed from the ST and are not claimed in this maintenance update because they are no longer considered valid products on the NIAP CCEVS Product Compliance List (PCL).

evaluated, and the APIs exposed to—and used by—the application have remained consistent. The Android client component executes essentially unchanged on these updated operating systems, with relatively minor code changes. Given the minor modifications to the Android client, the consistency of the APIs used by the client, and the positive results of the extensive regression testing conducted to ensure continued functionality, assurance is considered maintained for the updated platforms and operating systems.

Similarly, there is a single management API specification for iOS devices. Although the iOS client application only provides minimal functionality, extensive regression testing has been performed following modifications to accommodate changes to iOS. Therefore, assurance equivalence is maintained.

Changes to Evaluation Documents:
The following changes were made to the evaluation documents:

CC Evidence	Evidence Change Summary
Security Samsung SDS Co., LTD EMM (MDMPP20/MDMAEP20) Security Target, Version 0.4, 2016/12/22	Updated to identify the revised set of devices that can host the TOE agent and be managed by the TOE server
Design Documentation: See Security Target and Guidance	No changes required
Guidance Documentation: • Samsung SDS EMM Administrator's Guide, Version 1.5.1, December 2016 • Samsung SDS EMM Installation Guide, Version 1.5.1, December 2016 • Samsung SDS Push Installation Guide, Version 1.5.1, December 2016 • Samsung SDS AppTunnel Installation Guide, Version 1.5.1, December 2016	No significant changes have been made to any guidance documents.
Lifecycle: None	No changes required.
Testing: None	No changes required. Samsung SDS has performed regression testing on each newly supported device.
Vulnerability Assessment: None	The public search was updated from 6/30/2018. No public vulnerabilities exist in the product. See analysis results below.

Regression Testing:

Samsung SDS performed full regression testing of the updated Android agent application to ensure that it continues to run on each of the newly claimed phones. Samsung SDS also performed regression testing for the Samsung SDS iOS client, which is a non-security relevant component.

Vulnerability Analysis:

A vulnerability search from the time of the original evaluation (12/2016) and using most of the same terms was submitted as part of the IAR. Note that the mobile devices were excluded from the search since they have recently completed NIAP evaluations and both Apple and Samsung are addressing any published vulnerabilities on a regular (e.g., monthly) basis.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 6/30/2018 with the following search terms: "Crypto-J", "Samsung SDS", "Enterprise Mobility Management", "EMM", "CellWe" (the previous product name).

Database	Search Term	Matches	Identifiers	Disposition
VND	Crypto-J	0		
NVD	Crypto-J	2	CVE-2016-8217: EMC RSA BSAFE Crypto-J versions prior to 6.2.2 has a PKCS#12 Timing Attack Vulnerability. A possible timing attack could be carried out by modifying a PKCS#12 file that has an integrity MAC for which the password is not known. An attacker could then feed the modified PKCS#12 file to the toolkit and guess the current MAC one byte at a time. This is possible because Crypto-J uses a non-constant-time method to compare the stored MAC with the calculated MAC. This vulnerability is similar to the issue described in CVE-2015-2601. (https://nvd.nist.gov/vuln/detail/CVE-2016-8217)	Resolution: The TOE offers no interfaces to PKCS#12 files or any interface to the Crypto-J toolkit. As such, the identified issue is not exploitable in the evaluated configuration by any user who cannot already replace or change the entire TOE binary and configuration.
			CVE-2016-8212: An issue was discovered in EMC RSA BSAFE Crypto-J versions prior to 6.2.2. There is an Improper OCSP Validation Vulnerability. OCSP responses have two time values: thisUpdate and nextUpdate. These specify a validity period; however, both values are optional. Crypto-J treats the lack of a nextUpdate as indicating that the OCSP response is valid indefinitely instead of restricting its validity for a brief period surrounding the thisUpdate time. This vulnerability is similar to the issue described in CVE-2015-4748. (https://nvd.nist.gov/vuln/detail/CVE-2016-8212)	Resolution: The TOE doesn't use OCSP - it uses CRLs. As such, this issue is not exploitable or relevant in the evaluated configuration.
VND	Samsung SDS	0		
NVD	Samsung SDS	1	CVE-2017-10963	This match is related to other products and is not applicable to the TOE.
VND	Enterprise Mobility Management	0		
NVD	Enterprise Mobility Management	1	CVE-2017-10963	This match is a duplicate (see above).
VND	EMM	0		
NVD	EMM	16	CVE-2017-18269/ CVE-2018-11212/ CVE-2018-6639/ CVE-2017-14870/ CVE-2014-1859/ CVE-2017-14269/ CVE-2017-14268/ CVE-2017-14267/ CVE-2017-10929/ CVE-2017-9949/ CVE-2014-9961/ CVE-2017-5672/ CVE-2016-10114	13 matches are related to other products and are not applicable to the TOE.
			CVE-2017-10963	This match is a duplicate (see above).

Database	Search Term	Matches	Identifiers	Disposition
			CVE-2015-9167: In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Automobile and Snapdragon Mobile SD 410/12, SD 425, SD 430, SD 450, SD 600, SD 615/16/SD 415, SD 617, SD 625, SD 650/52, SD 800, SD 808, SD 810, SD 820, and SD 820A, in an EMM command, an integer underflow can occur. (https://nvd.nist.gov/vuln/detail/CVE-2015-9167)	Resolution: Samsung Feb 2018 patch
			CVE-2015-9143: In Android before 2018-04-05 or earlier security patch level on Qualcomm Snapdragon Mobile and Snapdragon Wear IPQ4019, MDM9206, MDM9607, MDM9615, MDM9625, MDM9640, MDM9650, MDM9655, MSM8909W, SD 210/SD 212/SD 205, SD 400, SD 410/12, SD 600, SD 615/16/SD 415, and SDX20, when reading CDT from eMMC with a very large meta offset (>size of default CDT-array compiled in bootloader) for one of the CDBs, a buffer overflow occurs. (https://nvd.nist.gov/vuln/detail/CVE-2015-9143)	Resolution: Samsung Feb 2018 patch
VND	CellWe	0		
NVD	CellWe	0		

Conclusion:

CCEVS reviewed the description of the changes and the analysis of their impact upon security and found them all to be minor. The changes to the server component have minimal impact on security, and the changes to the Knox container's numbering scheme are functional rather than security-relevant. The regression testing performed on the newly-claimed Android devices has confirmed that all security-relevant functionality still operates as evaluated on the originally claimed platforms. The updated vulnerability analysis did not uncover any additional known residual vulnerabilities that were unpatched. Therefore, CCEVS agrees that original assurance is maintained for the product.