ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Samsung SDS EMM v2.2.5

Maintenance Update of Samsung SDS EMM v2.2.5

Maintenance Report Number: CCEVS-VR-VID11013-2021

Date of Activity: April 26, 2021

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 v2.2.5, Revision 1.0, March 8, 2021
- Protection Profile for Mobile Device Management, Version 4.0, April 25, 2019
- Protection Profile for Mobile Device Management Agents, Version 1.0, April 25, 2019
- Functional Package for Transport Layer Security (TLS), Version 1.1, February 12, 2019

Documentation reported as being updated:

- Samsung SDS Co. Ltd. EMM and EMM Agent v2.2.5 for Android Security Target, Version 1.1, 8 March 2021

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 March 2021. 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:

The TOE has not been changed. Regression testing (testing the claimed management functions on added devices and otherwise determining correct operation of the TOE agent) has confirmed support for the added client devices. These Android 10 and iOS 13 devices were available when the TOE completed evaluation originally but had not completed their own evaluations against their applicable NIAP requirements. They were therefore excluded from scope and could not be claimed in the original TOE evaluation. Note that the TOE was designed to support those OS versions and subsequent regression testing has verified that the evaluated TOE can manage the devices which have now completed their evaluations – see the following PCL links:

- Android 10 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11109,
- Android 10 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11042, and
- iOS 13 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11036.

Note also that since the original evaluation some of the claimed mobile device evaluations have been removed from the NIAP PCL and hence are removed from the revised Security Target as identified here:

- Android 8.1 - https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10927,
- Android 8 - https://www.niap-ccevs.org/Product/Maint.cfm?AMID=427&PID=10898, and
- iOS 11 - https://www.niap-ccevs.org/Product/Maint.cfm?AMID=420&PID=10851).

Changes to the Development Environment

None, except that different managed devices are supported as identified previously in this report.

Changes to Evaluation Documents

This section provides a brief description of the modifications required to the affected CC evidence. For each item identified, the changes are described below:

1. Security Target – The Security Target has been updated to identify the revised set of devices that can host the TOE agent and be managed by the TOE server. Note that some newer devices were added and older devices were removed.

Changes to Evaluation Evidence

This section identifies all of the CC evidence that has been changed as a result of TOE modifications.

CC Evidence	Evidence Change Summary
Samsung SDS Co. Ltd. EMM and EMM Agent for Android Security Target, version 0.9, 01/27/2020	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, Solution version 2.2.5, January 2020 • Samsung SDS EMM Installation Guide, Solution version 2.2.5, January 2020 • Samsung SDS EMM Configuration Guide for IPsec settings in Microsoft Windows Server 2016 for Common Criteria Evaluation version 2.2.5, January 2020	No significant changes have been made to any guidance documents.
Lifecycle: None	No changes required.
Certificates None	No changes required. Certificate claims were not impacted.
Testing: None	No changes required. Samsung SDS has performed regression testing on each newly supported device.
Vulnerability Assessment: None	The public search was updated by the vendor from 01/27/2020 to 3/8.2021. The validation team updated this public search again from 3/8/2021 to 4/26/2021. No public vulnerabilities exist in the product. See analysis results below.

Vulnerability Analysis:

The evaluator performed a search for vulnerabilities from the time of the original evaluation (01/27/2020) and using most of the same terms. 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/), Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities), Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories), Exploit / Vulnerability Search Engine (http://www.exploitsearch.net), SecurITeam Exploit Search (http://www.securiteam.com)[1], Tenable Network Security (http://nessus.org/plugins/index.php?view=search), Offensive Security Exploit Database (https://www.exploit-db.com/) on 4/26/2021 with the following search terms: "RSA Crypto J", "Crypto-J", "CryptoJ", "Samsung SDS", "SDS", "Enterprise Mobility Management", "EMM".

[1] The Exploit / Vulnerability Search Engine appears to be down (Error 400 Bad Request) so this site was omitted from the search performed on 4/26. This site was included in the previous search reportedly performed by the vendor on 3/8.

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

Database	Search Term	Matches	Identifiers	Disposition
VND	RSA Crypto J	0		
NVD	RSA Crypto J	0		
VND	Crypto-J	0		
NVD	Crypto-J	0		
VND	CryptoJ	0		
NVD	CryptoJ	0		
VND	Samsung SDS	0		
NVD	Samsung SDS	0		
VND	SDS	0		
NVD	SDS	16	CVE-2021-21270/ CVE-2020-29478/ CVE-2020-12311/ CVE-2020-12310/ CVE-2020-12309/ CVE-2020-11184/ CVE-2020-14180/ CVE-2020-11985/ CVE-2020-11984/ CVE-2020-3180/ CVE-2020-14166/ CVE-2020-0527/ CVE-2020-7618/ CVE-2020-1927/ CVE-2020-1934/ CVE-2020-8664	16 matches are related to other products and are not applicable to the TOE.
VND	Enterprise Mobility Management	0		
NVD	Enterprise Mobility Management	0		
VND	EMM	2	VU#815128/ VU#231329	2 matches are related to other products and are not applicable to the TOE.
NVD	EMM	14	CVE-2020-26287/ CVE-2020-28926/ CVE-2018-20805/ CVE-2020-13799/ CVE-2020-3634/ CVE-2020-3491/ CVE-2020-13111/ CVE-2019-14020/ CVE-2020-11005/ CVE-2020-9337/ CVE-2020-9339/ CVE-2020-9338/ CVE-2020-9336/ CVE-2018-14553	14 matches are related to other products and are not applicable to the TOE.
Rapid7	RSA+Crypto+J	0		
ZDI	RSA Crypto J	0		
EXP	RSA+Crypto+J	0		
SIT	RSA Crypto J	0		
EDB	RSA Crypto J	0		
TEN	RSA Crypto J	0		
Rapid7	Crypto-J	0		
ZDI	Crypto-J	0		
EXP	Crypto-J	0		
SIT	Crypto-J	0		
EDB	Crypto-J	0		
TEN	Crypto-J	0		
Rapid7	CryptoJ	0		
ZDI	CryptoJ	0		
EXP	CryptoJ	0		
SIT	CryptoJ	0		
EDB	CryptoJ	0		
TEN	CryptoJ	0		
Rapid7	Samsung+SDS	0		
ZDI	Samsung SDS	0		
EXP	Samsung+SDS	0		
SIT	Samsung SDS	0		
EDB	Samsung SDS	0		
TEN	Samsung SDS	0		
Rapid7	SDS	0		
ZDI	SDS	0		
EXP	SDS	0		
SIT	SDS	1	0	This match is related to other products and is not applicable to the TOE.
EDB	SDS	0		
TEN	SDS	0		

Database	Search Term	Matches	Identifiers	Disposition
Rapid7	Enterprise+Mobility+ Management	0		
ZDI	Enterprise Mobility Management	0		
EXP	Enterprise+Mobility+ Management	0		
SIT	Enterprise Mobility Management	0		
EDB	Enterprise Mobility Management	0		
TEN	Enterprise Mobility Management	0		
Rapid7	EMM	0		
ZDI	EMM	0		
EXP	EMM	0		
SIT	EMM	0		
EDB	EMM	0		
TEN	EMM	0		

Conclusion:

CCEVS reviewed the description of the changes and find they have no impact upon security since the changes are only to documentation. The regression testing performed on the newly-claimed 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.