ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Samsung SDS Co. Ltd. EMM v2.2.5

Samsung SDS Co. Ltd. EMM v2.2.5

Maintenance Report Number: CCEVS-VR-VID11013-2022

Date of Activity: 14 April 2022

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 1.1, 31 March 2022
- Samsung SDS Co. Ltd. EMM and EMM Agent v2.2.5 for Android Security Target, Version 1.2, 8 March 2022
- Samsung SDS EMM Administrator's Guide, Solution version 2.2.5.5, November 2021
- Samsung SDS EMM Installation Guide, Solution version 2.2.5.5, November 2021
- Protection Profile for Mobile Device Management, Version 4.0, 25 April 2019
- PP-Module for MDM Agents, Version 1.0, 25 April 2019
- Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019

Assurance Continuity Maintenance Report:

Gossamer submitted an Impact Analysis Report (IAR) for the Samsung SDS EMM v2.2.5 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 8 March 2022. 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.

The evaluation evidence submitted for consideration consists of the Security Target, the Administrator's Guide, the Installation Guide, and the Impact Analysis Report (IAR). The ST, Admin Guide, Installation Guide and IAR were updated.

The updated documentation table, the minor change breakdown and the vulnerability analysis have all been pulled directly from the IAR.

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Samsung SDS Co. Ltd. EMM and EMM Agent for Android Security Target, version 0.9, 01/27/2020	Updated to identify the new TOE minor version number and 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	The administrator guide and installation guide have been revised to refer to the current product version and otherwise the install guide is revised to address licensing changes and also to add sections for upgrading the supporting Tomcat product and for adding and removing TOE patches while the admin guide has been revised to reference new unclaimed features referenced in the release notes. The IPsec configuration guide is unchanged.
Lifecycle: None	No changes required.
Testing: None	No changes required. Samsung SDS has performed regression testing on each newly supported device and operating system and have generally ensured the management functions continue to operate as claimed.
Vulnerability Assessment: None	The public search was updated from 01/27/2020 to 3/30/2022. No public vulnerabilities exist in the product. See analysis results below.

Changes to the TOE:
The changes are summarized below.

<u>Major Changes</u>

None.

Minor Changes

The TOE consists of server and client components for Android and iOS. Since the initial evaluation, support for the following devices has been dropped:

Evaluation Name	**Devices**
Samsung Galaxy Devices with Android 8 & 8.1 (VID10927)	Galaxy Note9
	Galaxy Tab S4
	Galaxy Tab S3
	Galaxy S7
	Galaxy S7 Edge
	Galaxy S7 Active
Samsung Galaxy Devices on Android 8 (VID10898)	Galaxy S9
	Galaxy S9+
	Galaxy Note8
	Galaxy S8
	Galaxy S8+
	Galaxy S8 Active
Apple iOS 11 (VID10851)	iPhone 5s
	iPhone 6 Plus/ iPhone 6
	iPhone 6s Plus/ iPhone 6s
	iPhone 7 Plus/ iPhone 7
	iPhone 8 Plus/ iPhone 8
	iPhone X
	iPhone SE
	iPad mini 3
	iPad mini 4
	iPad Air 2
	iPad Pro 12.9”
	iPad Pro 9.7”
	iPad
	iPad Pro 12.9”
	iPad Pro 10.5”
Samsung Galaxy Devices with Android 9 – Fall (VID11018)	Galaxy Note10
	Galaxy Note10 5G
	Galaxy Note10+
	Galaxy Note10+ 5G
	Galaxy Tab S3
	Galaxy Tab Active2
Samsung Galaxy Devices on Android 9 (VID10979)	Galaxy S10 5G
	Galaxy S10+
	Galaxy S10
	Galaxy S10e
	Galaxy Fold
	Galaxy Note9
	Galaxy Tab S4

	Galaxy S9+
	Galaxy S9
	Galaxy Note8
	Galaxy S8+
	Galaxy S8
	Galaxy S8 Active
Apple iOS 12 (VID10937)	iPhone 6
	iPhone 6 Plus
	iPad mini 4
	iPad Air 2
	iPhone 6s
	iPhone 6s Plus
	iPhone SE
	iPad 9.7-inch (5th generation)
	iPad Pro 12.9-inch
	iPad Pro 9.7-inch
	iPhone 7
	iPhone 7 Plus
	iPad 9.7-inch (6th generation)
	iPad Pro 12.9-inch (2nd generation)
	iPad Pro 10.5-inch
	iPhone 8
	iPhone 8 Plus
	iPhone X
	iPhone XS
	iPhone XS Max
	iPhone XR
	iPad Pro 11-inch
	iPad Pro 12.9-inch

As per the previous assurance continuity activity documented in "ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Samsung SDS EMM v2.2.5", CCEVS-VR-VID11013-2021, together with this assurance continuity activity, the final set of claimed supported evaluated devices is:

Evaluation Name	**Devices**
Samsung Galaxy Devices on Android 10 – Fall (VID11109)	Galaxy A71 5G
	Galaxy A51 5G
	Galaxy Tab Active3
	Galaxy Tab S4
Samsung Galaxy Devices on Android 10 – Spring (VID11042)	Galaxy S20 FE
	Galaxy Fold2
	Galaxy Fold 5G
	Galaxy Fold
	Galaxy Note20+ 5G

	Galaxy Note20+ LTE
	Galaxy Note20 5G
	Galaxy Note20 LTE
	Galaxy Tab S7+
	Galaxy Tab S7
	Galaxy Z Flip 5G
	Galaxy S20 Ultra 5G
	Galaxy S20+ 5G
	Galaxy S20+ LTE
	Galaxy S20 5G
	Galaxy S20 TE
	Galaxy S20 LTE
	Galaxy XCover Pro
	Galaxy A51
	Galaxy Note10+ 5G
	Galaxy Note10+
	Galaxy Note10 5G
	Galaxy Note10
	Galaxy Tab S6 5G
	Galaxy Tab S6
	Galaxy S10 5G
	Galaxy S10+
	Galaxy S10
	Galaxy S10e
	Galaxy Z Flip
	Galaxy Note9
	Galaxy XCover FieldPro
	Galaxy S9+
	Galaxy S9
Apple iOS 13 on iPhones and Apple iPadOS 13 on iPad Mobile Devices (VID11036)	iPad mini 4
	iPad Air 2
	iPhone 6s
	iPhone 6s Plus
	iPhone SE
	iPad 9.7-inch (5th gen)
	iPad Pro 12.9-inch
	iPad Pro 9.7-inch
	iPhone 7
	iPhone 7 Plus
	iPad 9.7-inch (6th gen)
	iPad 10.2-inch (7th gen)
	iPad Pro 12.9-inch (2nd gen)
	iPad Pro 10.5-inch
	iPhone 8
	iPhone 8 Plus

	iPhone X
	iPhone XS
	iPhone XS Max
	iPhone XR
	iPad mini (5th gen)
	10.5-inch iPad (3rd gen)
	11-inch iPad Pro
	12.9-inch iPad Pro
	11-inch iPad Pro (2nd gen)
	12.9-inch iPad Pro (4th gen)
	iPhone 11
	iPhone 11 Pro
	iPhone 11 Pro Max
	iPhone SE (2nd gen)
Samsung Galaxy Devices on Android 11 – Fall (VID11211)	Galaxy A52 5G
	Galaxy A42 5G
	Galaxy A71 5G
	Galaxy A51 5G
	Galaxy Tab Active3
Samsung Galaxy Devices on Android 11 – Spring (VID11160)	Galaxy S21+ 5G
	Galaxy S21 5G
	Galaxy S21 5G FE
	Galaxy Z Fold3 5G
	Galaxy Z Fold2 5G
	Galaxy Fold 5G
	Galaxy Fold
	Galaxy Z Flip3 5G
	Galaxy Z Flip 5G
	Galaxy Z Flip
	Galaxy Note20 Ultra 5G
	Galaxy Note20 Ultra LTE
	Galaxy Note20 5G
	Galaxy Note20 LTE
	Galaxy S20 Ultra 5G
	Galaxy S20+ LTE
	Galaxy S20 5G
	Galaxy S20 LTE
	Galaxy S20 FE
	Galaxy S20 TE
	Galaxy Tab S7+
	Galaxy Tab S7
	Galaxy Tab S6
	Galaxy A51
	Galaxy Note10+
	Galaxy Note10 5G

	Galaxy Note10+ 5G
	Galaxy Note10
	Galaxy S10+
	Galaxy S10 5G
	Galaxy S10
	Galaxy S10e
Apple iOS 14: iPhones (VID11146)	iPhone 6s
	iPhone 6s Plus
	iPhone SE
	iPhone 7
	iPhone 7 Plus
	iPhone 8
	iPhone 8 Plus
	iPhone X
	iPhone XS
	iPhone XS Max
	iPhone XR
	iPhone 11
	iPhone 11 Pro
	iPhone 11 Pro Max
	iPhone SE (2nd gen)
	iPhone 12 mini
	iPhone 12
	iPhone 12 Pro
	iPhone 12 Pro Max

In terms of actual product changes, the TOE has gone through a series of 5 release updates: 2.2.5.1, 2.2.5.2, 2.2.5.3, 2.2.5.4, and 2.2.5.5[1]. Samsung SDS has a corresponding series of release notes that summarize the new features and identify known issues. While the new features serve to identify changes, the known issues do not, although they could identify potential vulnerabilities. Please note, the features listed below are not covered by the evaluation since they have not undergone NIAP testing and are not claimed in the Security Target. Each of the release notes is summarized below.

High Security Release 2.2.5.1

- **[Agent] Direct Boot support (on Locked status)** – This change enables the Android agent to run during the initial power on, but not yet unlocked state. This has no impact on the claimed security functions of the TOE server or agent.
- **[Agent] Dual DAR (Data-at-rest) support** – This change adds the ability for the agent to support management of Knox container DualDAR functions. There are no claims for this

[1] Note that the release note versions 2.3.0, 2.3.5, 2.4, 2.4.1, and 2.4.5 are enterprise security revision numbers that correspond to the evaluated high security revision numbers 2.2.5.1, 2.2.5.2, 2.2.5.3, 2.2.5.4, and 2.2.5.5.

management function, so it is added functionality that does not impact any claimed or evaluated functions.

- **[Device] Certificate reinstall and enhancement** – There is an added check to ensure the Android agent and server versions match before X.509 certificates are accepted when provisioning (enrolling). This is an added check that is not related to a claimed security function. Additionally, the Android agent checks for upcoming certificate expirations and notifies the user. This also is not related to any claimed security function.
- **[UI/UX] Look & Feel Improvement** – This change involves some minor web interface screen changes and doesn't impact any security claims.
- **[Application] 'Need Update' status added for internal app** – This change to the web interface provides a new function that can check the version of actual applications installed on devices against the current application versions so an administrator can identify applications that are out of date. This is extra functionality not related to any claimed security function.
- **[Kiosk] Exit Kiosk mode** – This change allows a device that has been placed into kiosk mode to exit kiosk mode without being deactivated. This functionality is not related to any claimed security functions – note that kiosk mode was not specifically evaluated since it just restricts device functions and was considered out of scope for an enterprise deployment.
- **[Application] App installation and deletion API** – This change adds some Open APIs on the TOE web interface – these changes do not impact any security claims since they are just alternate names for already existing APIs that invoke the same corresponding underlying functions. The security checks and other behavior are within the underlying functions.
- **[Profile] Samsung Knox for Android Enterprise** – This change adds a new group for Samsung Knox specific security policies. It serves to change the organization of configurable policies in the web interface, but doesn't change the function of any security policies.
- **[iOS] Enhanced Device Enrollment Program (DEP)** – The DEP enrollment process is not changed, but this change allows an administrator to assign different users to each DEP enrolled device. Note that DEP enrollment was not evaluated and is out of scope.
- **[Console] MGP Auto update App setting** – This change allows the administrator to change the layout of Play Store information in the web interface. This presentational change is not related to any claimed security function.
- **[Console] Max. number of users per page** – This change increases the number of users that can be displayed per page on the web interface. This presentational change is not related to any claimed security function.
- **[Console] Device Column Customization** – This change allows the user to customize the device web interface page by showing and hiding selected columns. This presentational change is not related to any claimed security function.

- **[Console] Add app version in group and organization** – This change adds an app version column in group and organization screens so the administrator has direct access to that information on those screens. This presentational change is not related to any claimed security function.
- **[Profile] User Exceptional Profile Support** – This change adds the ability to create and assign temporary profiles to users. This is an unevaluated additional feature that doesn't impact any claimed security function.
- **[SecuCamera] SecuCamera for Samsung DeX / Tablet Support** – This adds support for a feature that is not related to any claimed security function.
- **[General] v2.3 Deprecated Feature** – This change removes support for a deprecated feature that is not related to any claimed security function.
- **Minor Enhancement: Profile** – This change allows an administrator to grant permissions for an app to install other configured apps. This is not related to any claimed security function.
- **Minor Enhancement: Devices** – These changes involve visual changes not related to any claimed security function and removal of an unclaimed QR-code log-in feature for affiliated products. None of these changes impact any claimed security function.
- **Minor Enhancement: Configuration** – The TOE server has been changed to accept a default setting to impose an 8 character minimum password rule and to include a setting that determines whether the IOS app inventory will be collected. These are unclaimed settings and as such do not impact any claimed security function.
- **Minor Enhancement: Other** – These are all minor visual changes in the web interface and do not impact any claimed security function.

There are several reported known issues for 2.2.5.1. A review of these issues indicates there are no reported security vulnerabilities but rather there are several functional limitations or conditions for the general operation of the product.

High Security Release 2.2.5.2

- **[Console] KPE-Standard / Premium license support** – This change addresses changes in product licensing and does not impact and claimed security function.
- **[Console] KPE-Premium multi-license support** – This change addresses changes in product licensing and does not impact and claimed security function.
- **[Configuration] Log file and database storage cycle** – This change supports some configuration for log retention and represents extra functions that do not impact any claimed security functions.
- **[Profile] Exporting profile policies as an Excel file** – This change adds a new function to export defined policies as Excel files. It's an added function that does not impact any claimed security function.

- **[GDPR] Terms and Policy support** – This change adds support for defining and displaying terms and consent notifications and is not related to any claimed security function.
- **[iOS] APNs token authentication support** – This change drops legacy support for iOS APNs tokens for authentication. That was not used in the original evaluation and does not impact any claimed security function.
- **[Configuration] Administrator password settings** – This change adds configuration settings for TOE administrators – minimum password length, maximum duration, and history settings. While these are security related, they are not related to any claimed security functions and serve as extra functions that will cause administrator passwords to be forced to change and limited in acceptability.
- **[Configuration] AhnLab V3 engine upload limit capacity expanded** – This change expands an upload limit, but for a feature that was not included in the evaluation so it has no impact on any claimed security function.
- **[Profile] File upload permission added in Kiosk Browser** – This change affects permissions for uploading files in kiosk mode. Kiosk mode was not included in the evaluation so this has no impact on claimed security functions.
- **[Device] Kiosk Browser UI change -** This affect changes the kiosk UI. Kiosk mode was not included in the evaluation so this has no impact on claimed security functions.
- **[Agent] Kiosk Browser/Remote Support/Secure Browser minimum version changed -** This affect changes the kiosk version support. Kiosk mode was not included in the evaluation so this has no impact on claimed security functions.
- **[Profile] Remote Support improved** – This change adds a time limit for remote support requests. This feature was not evaluated and does not impact any claimed security function.
- **[Device] sending the multiple app installation device command** – This change impact adds the ability to queue app installation so the administrator is not limited to installing one app at a time. The apps are still installed one at a time sequentially, so the function isn't really changed, just the interface to use it so there is no impact on any claimed security function.
- **[Device] Run app device command added for Android Enterprise devices** – This change adds the ability to run commands on certain devices. It is an added function that is not related to any claimed security function.
- **[Application] App icon WebP format extended** – This change adds the ability to associate more formats of icons with applications in the TOE web interface. It has no impact on any claimed security function.
- **[Device] Device's KME ID search added** – This change adds a search function on the TOE web interface device screens for KME IDs. This is not related to any claimed security function.

- **[Beta Service] Social Distancing monitoring** – This changed introduced an experimental social distancing capability that is unrelated to any claimed security functions.
- **[Migration] Profile setting components** – This change affects profile migration which does not impact any claimed security function.
- **[Others] Android 11 restrictions** – This change removes support for some deprecated legacy policy settings for non-Samsung Android devices and does not impact any claimed security function.
- **Minor Enhancements** – These changes are minor user interface changes, a in the content of a certificate template, removal of a deprecated configuration screen, and a fix to prevent an unexpected timeout – none of which impact any claimed security function.

There are several reported known issues for 2.2.5.2, many copied from 2.2.5.1. A review of these issues indicates there are no reported security vulnerabilities but rather there are several functional limitations or conditions for the general operation of the product.

High Security Release 2.2.5.3

- **[Console] App Configuration** – This change adds support for internal applications on a closed network allowing the administrator to configure the application settings rather than communicating with Google. This has no impact on any claimed security functions.
- **[Console] Smart Card sign-in support** – This change adds support for smart card login for administrators. This is an extra unclaimed function and while related to security, it out of scope and has no impact on any claimed security function.
- **[Console] Knox VPN Chaining** – This change adds support to configure dual VPNs. This is an extra function that has no impact on any claimed security function.
- **[Device] NFC permit control API change** – This change results in the use of an alternate API for a management function that did not work. This change has no impact on any claimed security function.
- **[Console] Inventory for checking device memory encryption added** – This change causes device and SD encryption status to be displayed in inventory details. This change is visual only and does not impact any claimed security function.
- **[Device] Application download message text changed** – This changes a status message from “transferring” to “downloading” on the managed device when downloading an app for installation. This has no impact on any claimed security function.
- **[Device] KPE Premium features available** – This change affects functions available depending on the licenses type (KPE-premium vs KPE-standard). It has no impact on any claimed security function.
- **[Others] Android 11 restrictions** – This change addresses the issues that serial numbers cannot be collected from legacy Android devices and KME activation no longer supports

Android Legacy mode. Legacy Android devices are out of scope and KME was not included in the evaluation. These changes do not impact any claimed security functions.

- **Minor Enhancements** – These changes address reading SIM card and serial number information from some devices and those changes do not impact any claimed security function. Also, any ADFS-based SSO logins will default to tenant ID and server domain information. This also is not related to any claimed security function since ADFS is out of scope of the evaluation.

There are several reported known issues for 2.2.5.3, the majority copied from 2.2.5.2. A review of these issues indicates there are no reported security vulnerabilities but rather there are several functional limitations or conditions for the general operation of the product.

High Security Release 2.2.5.4

- **[Console/Device]Work Profile on Company Owned device support** – This change adds specific support for managing Work Profiles on Company Owned devices. This is a mode of deployment not included in the original scope of evaluation and as such represents extra unclaimed functionality. It has no impact on any claimed security function.
- **[Console/Device]Android Enterprise Dual DAR support** - This change adds support for management of Knox container DualDAR functions on company owned devices. There are no claims for this management function or mode of operation, so it is added functionality that does not impact any claimed or evaluated functions.
- **[Console]IMEI/Serial Number support** – This change adds the ability to view IMEI/serial number information for certain devices and does not impact any claimed security function.
- **[Console]Duplicated Internal/public app package registration** support – This change adds support to allow multiple application packages with the same name and does not impact any claimed security function.
- **[Console]Device fields added in report** – This change adds device status about the device and SD card encryption to a set of reports that can be generated via the TOE web interface. This change has no impact on any claimed security function.
- **[Console]Improvement profile configuration audit** – This change adds a "Cause" field for profile related audit records. This extra information has no impact on any claimed security function.
- **[Console]Free KPE-Premium license** – This change adds support for free KLM/KPE licenses. This has no impact on any claimed security function.
- **Minor Enhancements** – These changes KLM licenses requirements, adds an additional method to get to offline deactivation to get past an identified issue, limits work profile enrollment in some cases. None of those changes impacts any claimed security function. While the TOE EMM server can run on server 2019, that is not claimed and as such does not impact any claimed security function.

There reported known issues for 2.2.5.4 are the same as for 2.2.5.3.

High Security Release 2.2.5.5

- **[Console]Bulk assignment of DEP** – This change allows a template of users mapped to device serial numbers to be uploaded to allow the automatic association of users to DEP enrolled devices as they are enrolled. This is essentially an unclaimed extra function that has no impact on any claimed security function.
- **[Console]Setting iOS DEP device name and EMM enrollment method** – This change supports the association of DEP device names with users and enrollment methods. Since DEP was out of scope for the evaluation, this is an extra function that has no impact on any claimed security function.
- **[Console]Improvement of iOS VPP application assignment** – This adds the ability to associated Apple VPP (Volume Purchase Program) apps with devices so not Apple ID is needed. VPP was out of scope for the evaluation and as such this in an extra function that has no impact on any claimed function
- **[Console]Bulk assignment of control applications support** – This change adds support to bulk add control applications. This change has no impact on any claimed security functions.
- **[Console/Device] Unassignment option while registering applications support** – This change causes application to be uninstalled automatically when unassigned. It has no impact on any claimed security function.
- **[Console/Device]Android Enterprise application event support** – This change adds an event for when certain applications run on a managed device. This is an extra event and does not impact any claimed security functions.
- **[Console]Android Enterprise web applications support** – This change adds support the Managed Google Play application to run in a Chrome browser. It is visual only and does not impact any claimed security function.
- **[Console/Device]XAPX files for Android internal applications support** – This change adds support for XAPK applications (that are bundles of two or more APKs) as internal apps loaded into the Google Play Store. They are not supported in the EMM application store, so this does not impact any claimed security function.
- **[Console/Device]Kiosk application whitelist policy support** – This change ensures that apps that are not on a white list will not run in Kiosk mode. Since Kiosk mode is not part of the evaluation this change has no impact on any claimed security function.
- **[Console]License deduction based on device activation** – This change causes available device license determination to be based on the number of activated and not just the number of registered devices. This change has no impact on any claimed security function.

- **[Console]Unit change of the iOS lock screen camera policy** – The camera control setting has moved from a global tenant-based setting to group and organization profiles. This more granular control has no impact on any claimed security function.
- **[Device]New firmware support** – This change supports iOS15 devices and Android 12 devices. However, at this point there are no corresponding evaluated devices from Apple or Samsung so this is extra functionality and does not impact any claimed security functions.
- **Android 12 restrictions** – These changes are based on different Android 12 behaviors related to the inability to capture screens when screens are protected by Android and to support new strongswan VPN settings. There are no evaluated Samsung Android 12 devices, so this has no impact on any claimed security functions.
- **Minor Enhancements** – These changes include ensuring that users registered in bulk have passwords configured that meet complexity requirements; adding extra information with Bluetooth UUIDs are black or white listed; microphone and camera permissions will not be requested by the device agent since they are not needed. None of these changes has an impact on any claimed security function.

There are several reported known issues for 2.2.5.5, the majority copied from 2.2.5.4. A review of these issues indicates there are no reported security vulnerabilities but rather there are several functional limitations or conditions for the general operation of the product.

Regression Testing:
Samsung SDS has performed regression testing on each newly supported device and operating system and have generally ensured the management functions continue to operate as claimed.

NIST CAVP Certificates:

Not Applicable

Vulnerability Analysis:
A search was performed for vulnerabilities from the time of the original evaluation (01/27/2020) and using most of the same terms on 3/1/2022 and subsequently updated on 3/30/2022. 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 table below shows the new search results from the 3/30/2022 analysis. The subsequent table shows results from the 3/1/2022 analysis.

The evaluator conducted the follow search on 3/30/2022. 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), Tenable Network Security

(http://nessus.org/plugins/index.php?view=search), Offensive Security Exploit Database (https://www.exploit-db.com/) on 3/30/2022 with the following search terms: "RSA Crypto J", "Crypto-J", "CryptoJ", "Samsung SDS", "SDS", "Enterprise Mobility Management", "EMM".

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	2	CVE-2022-27882 / CVE-2022-27881	2 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	0		
NVD	EMM	0		
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		

Database	Search Term	Matches	Identifiers	Disposition
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	0		
EDB	SDS	0		
TEN	SDS	0		
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		

The evaluator conducted the follow search on 3/01/2022. 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), Tenable Network Security

(http://nessus.org/plugins/index.php?view=search), Offensive Security Exploit Database (https://www.exploit-db.com/) on 3/1/2022 with the following search terms: "RSA Crypto J", "Crypto-J", "CryptoJ", "Samsung SDS", "SDS", "Enterprise Mobility Management", "EMM".

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	28	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 / CVE-2021-31597 / CVE-2021-39115 / CVE-2021-0640 / CVE-2020-36239 / CVE-2021-32761 / CVE-2021-43951 / CVE-2021-43949 / CVE-2021-43947 / CVE-2021-43943 / CVE-2021-43948 / CVE-2021-43950 / CVE-2022-22689	28 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 (https://www.kb.cert.org/vuls/id/815128) / VU#231329 (https://www.kb.cert.org/vuls/id/231329)	2 matches are related to other products and are not applicable to the TOE.

NVD	EMM	27	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 / CVE-2020-21990 / CVE-2021-1928 / CVE-2021-39254 / CVE-2021-34436 / CVE-2021-3246 / CVE-2021-27597 / CVE-2021-3520 / CVE-2021-46333 / CVE-2021-40148 / CVE-2022-0673 / CVE-2022-0672 / CVE-2022-0671 / CVE-2021-46313	27 matches are related to other products and are not applicable to the TOE.
Rapid7	RSA+Crypto+J	0		
ZDI	RSA Crypto J	0		
EDB	RSA Crypto J	0		
TEN	RSA Crypto J	0		
Rapid7	Crypto-J	0		
ZDI	Crypto-J	0		
EDB	Crypto-J	0		
TEN	Crypto-J	0		
Rapid7	CryptoJ	0		
ZDI	CryptoJ	0		
EDB	CryptoJ	0		
TEN	CryptoJ	0		
Rapid7	Samsung+SDS	0		
ZDI	Samsung SDS	0		
EDB	Samsung SDS	0		
TEN	Samsung SDS	0		
Rapid7	SDS	0		
ZDI	SDS	0		
EDB	SDS	0		
TEN	SDS	0		
Rapid7	Enterprise+Mobility+Management	0		
ZDI	Enterprise Mobility Management	0		

EDB	Enterprise Mobility Management	0		
TEN	Enterprise Mobility Management	0		
Rapid7	EMM	0		
ZDI	EMM	0		
EDB	EMM	0		
TEN	EMM	0		

Conclusion:

The overall impact is minor. This is based on the rationale that updates do not change any security policies of the TOE and are unrelated from SFR claims. The updates described above were made to support the new TOE minor version number and the revised set of devices that can host the TOE agent and be managed by the TOE server.

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