T

# ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 11 – Spring.

## Maintenance Update of Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 11 – Spring.

**Maintenance Report Number: CCEVS-VR-VID11160-2022**

**Date of Activity**: 25 February 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 Electronics Co., Ltd. Samsung Galaxy Devices on Android 11 – Spring, Version 1.6, 21 February 2022,

**Documentation Updated**:

The original documentation has been updated to the following

**Security Target:** The Security Target was updated to include the new devices in the list of equivalent devices.

- Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 11 – Spring Security Target, version 1.1, December 15, 2021
- Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 11 - Spring Key Management Description, version 1.1, December 15, 2021

**Guidance Documentation**: A new administration guide document was produced to list the new devices.

- Samsung Android 11 on Galaxy Devices Administrator Guide, version 7.1, June 2, 2021
- A new application list has been created and posted to: https://support.samsungknox.com/hc/en-us/articles/115015195728-Common-Criteria-Mode.

**Assurance Continuity Maintenance Report:**

Gossamer Laboratories submitted an Impact Analysis Report (IAR) and Assurance Continuity Maintenance package on behalf of Samsung to the CCEVS for approval on July 29, 2021. There were several revisions with the final update submitted on 21 February 2022. The IAR is intended to satisfy the 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 new devices covered by this IAR are added as equivalent devices to the evaluated devices of the Galaxy S21+ 5G and Galaxy S21 5G (Qualcomm) shown in the entry row for **Galaxy S21 Ultra 5G** in the following table**.** The specific equivalent additions are highlighted in yellow in the table below. All non-highlighted devices in the table were included in the previous Assurance Maintenance action documented in CCEVS-VR-VID11160-2021, 3/15/2022.

| Evaluated Device | SoC | Equivalent Devices | Differences |
|---|---|---|---|
| **Galaxy S21 Ultra 5G** | Exynos 2100 | Galaxy S21+ 5G | S21 Ultra > S21+ > S21 in terms of display size |
| | | Galaxy S21 5G | S21+ & S21 devices have S20+ 5G Wi-Fi chip |
| **Galaxy S21 Ultra 5G** | Snapdragon 888 | Galaxy S21+ 5G | S21 Ultra > S21+ > S21 > in terms of display size |
| | | Galaxy S21 5G | S21+ & S21 devices have S20+ 5G Wi-Fi chip |
| | | Galaxy S21 5G FE | Z Fold3 5G & Z Flip3 5G have 2 displays & folding display |
| | | Galaxy Z Fold3 5G | Z Fold3 5G & Z Flip3 5G have power button fingerprint sensor |
| | | Galaxy Z Flip3 5G | Z Fold3 & Z Flip3 have different Wi-Fi chips |
| **Galaxy S20+ 5G** | Exynos 990 | Galaxy Note20 Ultra 5G | S20 Ultra > S20+ > S20 > S20 FE in terms of display size |
| | | Galaxy Note20 Ultra LTE | |
| | | Galaxy Note20 5G | 5G devices have different cellular modem |
| | | Galaxy Note20 LTE | |
| | | Galaxy S20 Ultra 5G | Note20 Ultra > Note20 in terms of display size |
| | | Galaxy S20+ LTE | |
| | | Galaxy S20 5G | Note20 devices include S Pen & functionality to take advantage of it for input (not security related) |
| | | Galaxy S20 LTE | |
| | | Galaxy S20 FE | |
| **Galaxy S20+ 5G** | Snapdragon 865 | Galaxy Z Fold2 5G | S20 Ultra > S20+ > S20 > S20 FE in terms of display size |
| | | Galaxy Note20 Ultra 5G | Note20 Ultra > Note20 in terms of display size |

| Evaluated Device | SoC | Equivalent Devices | Differences |
|---|---|---|---|
| | | Galaxy Note20 5G | Note20 devices include S Pen & functionality to take advantage of it for input (not security related) |
| | | Galaxy Tab S7+ | Z Fold2 5G & Z Flip have 2 displays & folding display |
| | | Galaxy Tab S7 | Tab S7 devices are tablets (no voice calling) with S Pen |
| | | Galaxy Z Flip 5G | Tx70 tablets only have Wi-Fi, others have cellular |
| | | Galaxy S20 Ultra 5G | Tab S7+ > Tab S7 in terms of display size |
| | | Galaxy S20 5G | Tab S7+ & S20 FE have under screen image fingerprint sensor |
| | | Galaxy S20 TE | Tab S7, Z Fold2 5G & Z Flip 5G have power button fingerprint sensor |
| | | Galaxy S20 FE | |
| **Galaxy XCover Pro** | Exynos 9611 | Galaxy A51 | XCover Pro is ruggedized |
| | | | XCover Pro has Push-to-Talk button |
| | | | XCover Pro has removable battery |
| | | | A51 has under screen image fingerprint sensor |
| **Galaxy Note10+ 5G** | Exynos 9825 | Galaxy Note10+ | Note10+ > Note10 in terms of display size |
| | | Galaxy Note10 5G | 5G devices have different cellular modem |
| | | Galaxy Note10 | |
| **Galaxy S10e** | Exynos 9820 | Galaxy S10+ | S10 & S10+ have ultrasonic fingerprint sensor |
| | | Galaxy S10 5G | S10+ > S10 > S10e in terms of display sizes |
| | | Galaxy S10 | S10 5G has different cellular modem |
| **Galaxy S10+** | Snapdragon 855 | Galaxy Note10+ 5G | S10e, Fold & Z Flip have power button image fingerprint sensor |
| | | Galaxy Note10+ | S10 & S10e have smaller display sizes |
| | | Galaxy Note10 | 5G devices have different cellular modem |
| | | Galaxy Tab S6 | Fold & Z Flip have 2 displays |
| | | Galaxy S10 5G | Fold & Z Flip have folding display |
| | | Galaxy S10 | Note10+ > Note10 in terms of display size |
| | | Galaxy S10e | Note10 devices include S Pen & functionality to take advantage of it for input (not security related) |
| | | Galaxy Fold 5G | Tab S6 is tablet (no voice calling) with S Pen |
| | | Galaxy Fold | T867 & T865 tablets have LTE, T860 tablets only have Wi-Fi |
| | | Galaxy Z Flip | Tab S6 has under screen image fingerprint sensor |

The following table lists differences from the common hardware model **Galaxy S21 Ultra 5G.** The TOE software is identical on all models, and changes are based on the differences in the hardware components where there are variations from the previously certified model. Changes related to utilizing two screens on the new devices are outside the boundary of the TOE software (and hardware).

| Certified Model | Equivalent Model highlighted in first table | Differences in Equivalent Model |
|---|---|---|
| **Galaxy S21 Ultra 5G** | Galaxy Z Fold3 5G | • Two displays – one when closed, a folding display (7-8”) when opened (only one display is active at a time)<br>• Power button fingerprint sensor (this sensor is marked as fingerprint-I in the Security Target and evaluated on the S10e)<br>• Different Wi-Fi chip (see section **Error! Reference source not found.**) |
| **Galaxy S21 Ultra 5G** | Galaxy Z Flip3 5G | • Two displays – one when closed for notifications, a folding display (5-6”) when opened (only one display is active at a time)<br>• Power button fingerprint sensor (this sensor is marked as fingerprint-I in the Security Target and evaluated on the S10e)<br>• Different Wi-Fi chip (see section **Error! Reference source not found.**) |
| **Galaxy S21 Ultra 5G** | Galaxy S21 FE 5G | • Smaller screen size, lower resolution<br>• Smaller battery, flash storage |

The security software portion of the TOE boundary, as defined in the TSF Inventory section of the *Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 11 - Spring Key Management Description, version 1.1,* December 15, 2021, is identical between all models. There are no additional security features in the new devices, all changes are outside the core components of the TOE.

The S20 FE device models added as part of this maintenance action differ from the earlier S20 series devices in screen size and screen resolution. The added devices represent a minor change to the TOE.

### TOE Software Updates:

The TOE Software is identical on all models, except for the added support for the two displays. Software changes related to utilizing two screens on the new devices are not security relevant – the hardware is in the TOE boundary, but the actual display is not security relevant and judged to be minor.

All other software changes made to the TOE were to patch CVEs and Samsung Vulnerabilities and Exposures (SVEs). The searches and patches for known vulnerabilities listed in the IAR date back to March 2021, July 2021, October 12, 2021, December 15, 2021, and more recently February 21, 2022.

The following sites were used for the search for known vulnerabilities.

- Carnegie Mellon University - https://www.kb.cert.org/vuls/search/
- National Vulnerability Database - https://nvd.nist.gov/vuln/search

The following terms were used for the search.

- Samsung
    - Mobile
    - Semiconductor
    - Electronics
    - S20
    - S21
    - S10
    - Note20
    - Note10
    - XCover
- SM-G998
- SM-G986
- SM-G975
- SM-G970
- SM-N976
- SM-G715
- Android
- Strongswan
- Charon
- BoringSSL

Broad categories of the several hundred CVEs found are: Applications, Frameworks, Media Frameworks, Google-Play Services, Wildvine DRM, Android Runtime, System, Kernels, Qualcomm chipset components, Samsung chipset components.

All patched vulnerabilities are classified as minor fixes in terms of the evaluated TOE. To reach that conclusion, Samsung read and analyzed each vulnerability to ensure it did not directly impact

an SFR. Consideration was placed on what change was made and how it impacted a TOE component.

**Cryptography:**

The only differences in cryptographic certificates between the existing devices and the new equivalent devices are the Wi-Fi chipset. The Z Fold3 5G and the Z Flip3 5G have Qualcomm Wi-Fi chips based on the Lithium AES engine. These chips are certified with the AES algorithm cert 5663. The Wi-Fi software on all devices is identical.

| Device | Wi-Fi Chipset | Wi-Fi Alliance Certs |
|---|---|---|
| **Z Fold3 5G** | Qualcomm QCA6391 (Lithium) | 112366, 112269, 112362, 112365, 113087, 112364, 113086 |
| **Z Flip3 5G** | Qualcomm WCN6850 (Lithium) | 112311, 112263, 112329, 112328, 112327, 112326 |

**Regression testing:**

The development and testing of the certified components are set with the initial certification process. All updates, whether that is new devices on equivalent hardware or software patches, must undergo the same set of tests before being accepted for release. Tests include both unit testing of the components as well as quality assurance testing of the entire device. The components needed for certification are tested on all supported devices as part of the normal development and release process.

**Conclusion:**

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