ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 12 – Fall

---

Maintenance Update of Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 12 – Fall

Maintenance Report Number: CCEVS-VR-VID11307-2023

Date of Activity: 31 March 2023

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 12 - Fall, Revision 1.0, 10 March 2023.
- PP-Configuration for Mobile Device Fundamentals, Virtual Private Network (VPN) Clients, and Bluetooth, 15 May 2022 (CFG_MDF-VPNC-BT_V1.0)
    - The PP-Configuration includes the following components:
        - Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.2, (PP_MD_V3.2)
        - PP-Module: PP-Module for Virtual Private Network (VPN) Clients, Version 2.3, (MOD_VPNC-MDF_V2.3)
        - PP-Module: PP-Module for Bluetooth, Version 1.0, (MOD_BT_V1.0)
- General Purpose Operating Systems Protection Profile/Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, Version 1.0, 08 February 2016 (PP_WLAN_CLI_EP_V1.0)
- Functional Package: Functional Package for Transport Layer Security (TLS), Version 1.1, (PKG_TLS_V1.1)

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Evaluated Security Target: Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 12 – Fall Security Target, 03/24/2022, Version 0.4	**Current Maintained Security Target:** Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 12 – Fall Security Target, 03/10/2023, Version 0.5 Changed the maintained ST to remove the Galaxy Flip and A53 devices, any notes in the ST about these devices not supporting SD cards, and the associated CAVP algorithm certificate numbers.
Evaluated Common Criteria Guidance Documentation: Samsung Android 13 on Galaxy Devices Administrator Guide, version 8.0.1, October 24, 2022	**Maintained Common Criteria Guidance Documentation:** Samsung Android 13 on Galaxy Devices Administrator Guide, version 8.0.2, March 10, 2023 Updated to remove the Galaxy Flip and A53 devices and the note that stated these devices do not support SD cards.

Assurance Continuity Maintenance Report:

Samsung Electronics Co., Ltd. submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 22 March 2023. 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 consists of the Security Target, the Administrative Guide, and the Impact Analysis Report (IAR). The ST and guide document were updated, the IAR was new.

Changes to TOE:

There have been no product changes. The sole purpose for this maintenance action is to remove the Galaxy Z Flip4 and Galaxy A53 devices and associated equivalent devices. This was agreed upon between Samsung and NIAP to address a concern with the Linux kernel's use of Cha Cha 20 for entropy. These devices have been added to Samsung's Android 13 evaluation.

Software Changes

There have been no changes to the software.

Changes to Evaluation Documents:

1. Security Target – The Security Target has been updated to remove the Galaxy Flip and A53 devices.
2. Guidance document – The Admin Guide has been updated to remove the Galaxy Flip and A53 devices.

Regression Testing:

No regression testing was done.

Vulnerability Analysis:

CCTL stated that Samsung continually tracks bugs, vulnerabilities, and other defects reported in the public domain and as of 3/10/2023 there are no known outstanding security-related vulnerabilities in the TOE.

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. No functionality, as defined in the SFRs, was impacted, and there were no software updates. Thus, there were no changes to the security functionality or the SFRs identified in the Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.