CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Samsung Electronics Co., Ltd. Samsung Galaxy Devices with Qualcomm Snapdragon Processors (MDFPP10)

Maintenance Report Number: CCEVS-VR-VID10556-2014a

Date of Activity: 13 June 2014

References:

Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 2, September 8, 2008

Common Criteria document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements” Version 1, February 2004

Impact Analysis Report for Samsung Electronics Co., Ltd. Samsung Galaxy Devices with Qualcomm Snapdragon Processors (MDFPP10, Version 2.0, June 6, 2014

Samsung Electronics Co., Ltd. Samsung Galaxy Devices with Qualcomm Snapdragon Processors (MDFPP10) Security Target, Version 1.0, February 24, 2014

Evaluation Technical Report for Samsung Galaxy Devices with Qualcomm Snapdragon Processors (MDFPP10) (Proprietary), Version 5.0, February 24, 2014

Common Criteria Evaluation and Validation Scheme Validation Report Samsung Electronics Co., Ltd. Samsung Galaxy Devices with Qualcomm Snapdragon Processors, CR Version 0.5, February 26, 2014 (CR Report #: CCEVS-VR-10556-2014

Affected Evidence:

Samsung Electronics Co., Ltd. Samsung Galaxy Devices with Qualcomm Snapdragon Processors (MDFPP10) Security Target, Version 1.1, April 30, 2014

Samsung Electronics Co., Ltd. Samsung Galaxy Devices with Qualcomm Snapdragon Processors (MDFPP10) Security Target, Version 1.1, April 30, 2014

Samsung Android 4.4 on Galaxy Devices with Qualcomm Processors Guidance Documentation, version 0.11, 20 February 2014

Samsung Android 4.4 on Galaxy Devices with Qualcomm Processors User Guidance Documentation, version 0.11, 20 February 2014

Updated Developer Evidence:

Samsung Electronics Co., Ltd. Samsung Galaxy Devices with Qualcomm Snapdragon Processors (MDFPP11) Security Target, Version 1.1, 04/30/2014

Samsung Android 4.4 on Galaxy Devices Guidance Documentation, Version 1.5, April 30, 2014

Samsung Android 4.4 on Galaxy Devices User Guidance Documentation, Version 1.2, April 29, 2014

Assurance Continuity Maintenance Report:

Gossamer Laboratories CCTL, on behalf of Samsung Electronics Co., Ltd. submitted an Impact Analysis Report to CCEVS for approval. 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 2, September 8, 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence that was updated as a result of those changes, and the security impact of those changes.

Changes to TOE:

The TOE has been updated in the following areas.

1. Added support for VPN Client

   The security functionality surrounding the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013 (IVPNCPP) was added to the TOE.

   Assessment: All IVPNCPP functionality has been addressed (e.g., tested) in the context of a separate evaluation identifying the TOE devices as they are identified in this IAR. No additional or modified security claims are being made in regard to the originally evaluated ST.

2. GPS Bug fix

   When an application that uses GPS is not closed and the GPS is turned off by the user, Carrier IQ is unable to acquire GPS and keeps searching for a GPS signal continuously. This results in significant battery drain.

   Assessment: This change is functional in nature. It addresses a battery use issue but do not introduce any new security functions or alter the operation of claimed security functions.

3. BIP channel closes during ISIS

   The sendsocket close notification has been updated to be activated only after moving to CLOSDED state and not from TIME_WAIT state.

   Assessment: This change is functional in nature. It addresses a transmission issue over an intermediate system to intermediate system issue but does not introduce any new security functions or alter the operation of claimed security functions

4. LTE disable timer fix

   The timer associated with the LTE disable function incorrectly mapped 12 minutes to 6 minutes. The timing was corrected.

   Assessment: This change is functional in nature. It addresses a timing issue for disabling LTE functions but does not introduce any new security functions or alter the operation of claimed security functions

5. Samsung application updates

   These changes deal with the presentation of the default Samsung apps. Examples of such changes are changing the appearance of the Google application icon, in Camera app location of settings icon is changed, and the mail folders show total number of email not unread so the count was updated.

   Assessment: These changes are functional in nature. They only affect non-security relevant applications.

6. Carrier specific fixes

   Samsung implemented a set of carrier specific fixes that addressed such things as Beats music and ISIS Wallet are now installed by default.

   Assessment: These changes are functional in nature. They only affect non-security relevant applications.

Vendor Conclusion:

The changes consist of the addition of VPN Client support and some non-security relevant bug fixes. The VPN Client support has been addressed in a separate evaluation. This assurance continuity effort is to ensure the platform is current with the VPN Client evaluation.

The small number of bug fixes addresses functional issues and as indicated above none is related to the security claims in the evaluated ST.

The evaluation evidence consists of the Security Target administrator guidance, and user guidance. The Security Target was revised to identify the new product version. Likewise, the guidance documents were revised to identify the new product version.

Note that Samsung continually tracks bugs, vulnerabilities, and other defects reported in the public domain and at the time of this report there are no known outstanding security-related vulnerabilities in the TOE.

Validation Team Conclusion:

One change to the TOE did impact security functionality; the addition of VPN Client support. The vendor asserted that the added functionality had been tested under a separate evaluation conducted against the TOE devices identified herein. The validators confirmed that the testing of the VPN functionality was included in the evidence presented for VID10557.

The validation teams reviewed the changes and concurs that the changes are minor and not security relevant, with the one exception noted above; and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.