ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Samsung Electronics Co., Ltd. Samsung Galaxy S9 Tactical Edition (MDFPP31/WLANCEP10/VPNC21)

Maintenance Update of Samsung Electronics Co., Ltd. Samsung Galaxy S9 Tactical Edition (MDFPP31/WLANCEP10/VPNC21)

Maintenance Report Number: CCEVS-VR-VID10898-2018

Date of Activity: 18 October 2018

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;

Impact Analysis Report for Samsung Electronics Co., Ltd. Samsung Galaxy S9 Tactical Edition (MDFPP31/WLANCEP10/VPNC21), Version 1.1, October 12, 2018

Documentation reported as being updated:

- A new application list has been created and has been posted to https://support.samsungknox.com/hc/en-us/articles/115015195728-Common-Criteria-Mode.

Assurance Continuity Maintenance Report:

Samsung Electronics Co., Ltd. submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 18 September 2018, and revised on October 12, 2018. 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 2.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

The IAR identifies that the device is identical in hardware to the SM-G960U but with a modified system image not available on a standard, off-the-shelf device. The modified system image does not contain any security changes to the device. The IAR identifies the non-security related changes to the TOE as changes that center on SIM card usage, additional configuration options for networking and user input, and the removal of apps that will not be used in the deployed environments. The only security-related changes to the TOE include patches for software updates for vulnerabilities that are prepared as required by various policies and MDF requirements. The non-security related changes identified above were determined to be outside the scope of the MDF evaluation.

From the documentation relevant to the TOE, only the application list on the website listed above was new and added, as well as the IAR.

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.

Changes to TOE:

The specific device in question is a new variation of the Galaxy S9 (SM-G960U). The S9 Tactical Edition (SM-G960U, device build G960UZKAN14) is designed to meet the requirements for Tactical deployments. The device is identical hardware to SM-G960U but with a modified system image. No documentation updates were made for the new device except for the addition of the Application List in the website above. The non-security related changes that were made to the device center on SIM card usage, additional configuration options for networking and user input, and the removal of pre-installed apps. The changes and effects of additional features and support are summarized below.

1. SIM card & Network configuration

Security Consideration	Assessment
• SIM card configuration o Within the US only an AT&T SIM is allowed o Global Roaming with AT&T SIM is supported o Outside of the US, regional SIM cards can be used o All pop-ups related to the SIM such as when the SIM card is removed will not appear	This is not security relevant because the claimed and tested MDF functionality remains the same.
• Network related Settings o Multiple Ethernet interfaces are supported at once (up to 2) o IP shell commands to configure Ethernet settings at the Linux layer	Multiple Ethernet interface support and additional command line settings do not affect the security functionality of the device as the claimed and tested MDF functionality remains the same.
• New Management APIs to perform the following: o The ability to turn off/block all cellular network access	This is not security relevant because the claimed and tested MDF functionality remains the same.

o The ability to enable glove mode features (screen sensitivity) o The ability to remap the Bixby hardware button	

2. Pre-installed apps

Security Consideration	Assessment
Pre-installed apps from the SM-G960U device removed	Pre-installed apps are provided by device manufacturers, OS developers, and mobile carriers. They provide capabilities outside of scope and do not provide security functionality mandated by the MDF PP. Therefore, the removal of these pre-installed apps does not affect the original assurance of the product.

3. General Security Updates

Security Consideration	Assessment
The S9 Tactical Edition will receive regular security updates based on a modified release cycle. The devices are generally expected to only attach to closed networks and not directly to the internet, even when connecting via cellular service (the expected deployments generally utilize dedicated cellular APNs or Always-on VPN configurations to limit exposure). The base device for the S9 Tactical Edition device receives regular updates to maintain the overall security of the system as expected under a Common Criteria evaluation. Samsung works with Google to create update packages on a monthly basis for deployment. Updates for the S9 Tactical Edition would be based on the current update level at the time the update is created. Updates for the S9 Tactical Edition are planned every 6 months and will be made available directly from Samsung to customers of the device. These updates can be deployed either through physical	This is consistent with all applicable NIAP policies and MDF requirements related to vulnerabilities. The updates being delivered are direct from the vendor, consistent with the claims given in the IAR. Thus, original assurance is maintained.

flashing or by FOTA (if the customer has the capability to perform such deployments). Additional updates may be generated and provided as needed based on the severity of a chosen CVE. Samsung reviews the CVE database and prepares patches for applicable vulnerabilities on a regular basis and adds these into the SMRs for deployment during these updates.	

Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security, and found them all to be minor.

The S9 Tactical Edition includes the Android security patch level from September 1, 2018. The mobile device vendor reported having conducted a vulnerability search update that located no new vulnerabilities as reflected by update newsletters by the platform and mobile device vendors. Further it was also reported that the Vendor did regression testing through the normal Samsung QA process and early testing with DISA, and that the changes, collectively, no security impact on the TOE.

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