ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Apple iPad and iPhone Mobile Devices with iOS 11.2

Maintenance Update for: Apple iPad and iPhone Mobile Devices with iOS 11.2

Maintenance Report Number: CCEVS-VR-VID10851-2018a

Date of Activity: 17 July 2018

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008
- Apple Inc. Impact Analysis Report (IAR), CCEVS VID10851 Version 2.0,2018-07-13;
- Protection Profile for Mobile Device Fundamentals, Version 3.1, dated 16 June, 2017 [PP_MD_V3.1]
- Extended Package for Mobile Device Management Agents Version 3.0, dated 21 November, 2016 [EP_MDM_AGENT_V3.0]
- General Purpose Operating Systems Protection Profile/ Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients, dated 8 February, 2016 [PP_WLAN_CLI_EP_V1.0]
- Apple iPad and iPhone Mobile Devices with iOS 11.2 PP_MD_v3.1, EP_MDM_AGENT_V3.0 & PP_WLAN_CLI_EP_V1.0 Security Target Version 1.01 2018-03-30
- Apple iPad and iPhone Mobile Devices with iOS 11.2 PP_MD_v3.1, EP_MDM_AGENT_V3.0 & PP_WLAN_CLI_EP_V1.0 Common Criteria Guide, Version 1.01. 2018-3-30

Documentation reported as being updated:

- Security Target (Updated to Version 2.0, 2018-07-12)
- Common Criteria Guide (Updated to Version 2.0, 2018-07-12)

Assurance Continuity Maintenance Report:

Apple Inc, submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 25 June 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 any changes made to the certified TOE, any evidence updated because of the changes, and the security impact of any changes.

Introduction:

VID10851 Apple iPad and iPhone Mobile Devices with iOS 11.2 was evaluated by atsec information security Corporation for Apple Inc. on 2018-03-30. The products met the requirements specified by NIAP-approved protection profiles and extended packages PP_MD_V3.1, EP_MDM_AGENT_V3.0, and PP_WLAN_CLI_EP_V1.0.

The purpose of this document is to request the following three additional Apple iPad device models be included as platforms covered by VID10851.

1. 2018 iPad 9.7-inch, model A1893 (wifi only)
2. 2018 iPad 9.7-inch, model A1954 (wifi+cellular)
3. 2016 iPad Pro 9.7-inch, model A1675

Device models 1 and 2 are a new iPad 9.7-inch device that was not released in time to be included in the evaluation. Device model 3 was mistakenly omitted from the device list provided by the vendor.

Summary Description:

The Apple iPad 9.7-inch (models A1893 and A1954) released in 2018 a few days before the TOE was validated and therefore could not be included in the evaluation. These devices run the latest version of iOS 11 and contain the A10 Fusion processor, the same processor used by the iPhone 7 and iPhone 7 Plus that were included in the testing for the evaluation.

The Apple iPad Pro 9.7-inch (model A1675) released in 2016 and was intended to have been included in the evaluation. This omission was discovered in the process of gathering information to add the 2018 iPad 9.7-inch described above. The 2016 iPad Pro 9.7-inch runs the latest version of iOS 11 and contains the A9X processor, the same processor used by the other iPad Pro 9.7-inch models (A1673 and A1674) that were included in the evaluation.

No security relevant changes were made to the TOE hardware, the inclusion of the additional hardware devices does not change any of the security functions that are claimed in the Security Target. The hardware models added are to an existing series of evaluated and supported models. As the additional models use the same processors as devices tested under the VID10851 evaluation, no new NIST CAVP certificates are required.

Since the evaluation was completed, several minor updates of iOS have been released as normal maintenance updates to iOS. Each of those updates included security-related fixes. All publicly

disclosed vulnerabilities applicable to the TOE since the evaluation have been mitigated in the subsequent maintenance updates.

The evaluation evidence consists of the Impact Analysis Report (IAR) and supporting vulnerability analysis update, dated July 11, 2018.

The original evaluation was performed against the collaborative Protection Profile for Network Devices Version 1.0 and the ST referenced validated CAVP certificates. No changes were made to the processor and therefore no modifications were required to any of the valid NIST certificates.

Changes to TOE:
Additional hardware devices added to the supported device list. WiFi Alliance certificates were obtained for the new device models A1893 and A1954; WFA76387 and WFA76394 respectively.

Affected Developer Evidence:
None

Regression Testing:
The vendor performed regression testing to ensure correct operation of the hardware and software as a matter of course.

Vulnerability Analysis:
A new CVE search was conducted on 2018-07-11 using the same search terms and web sites used in the search performed VID10851 and no outstanding vulnerabilities were found related to the devices.

Conclusion:
CCEVS reviewed the vendor provided description of the analysis of the devices, and found there to be no impact upon security related functionality. In addition, the TOE vendor reported having conducted a vulnerability search update that located no new applicable vulnerabilities requiring mitigation that were not already resolved through the vendors update processes. All the security functions claimed in the ST remain enforced. Therefore, CCEVS agrees that the original assurance is maintained for the product.