ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Apple Inc. iPad and iPhone Mobile Devices with iOS 12

Maintenance Update for: Apple iPad and iPhone Mobile Devices with iOS 12.

Maintenance Report Number: CCEVS-VR-VID10937-2019

Date of Activity: 22 April 2019

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- Mobile Device Fundamentals Protection Profile, Version 3.1, dated 16 June 2017;
  - Extended Package for Mobile Device Management Agents, Version 3.0, dated 21 November 2016;
  - General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package Wireless Local Area Network {WLAN} Clients, Version 1.0, dated 8 February 2016
  - The PP-Module for Virtual Private Network {VPN} Clients, Version 2.1, dated 5 October 2017
- Apple Inc., Impact Analysis Report (IAR) VID10937, Version 1.0, 2019-04-17
- Apple iPad and iPhone Mobile Devices with iOS 12 Security Target, PP PP_MD_V3.1 with EP_MDM_AGENT_V3.0, PPWLAN_CLI_EP_V1.0, MOD_VPN_CLI_V2.1, Version 1.6, 2019-03-12.
- Common Criteria Evaluation and Validation Scheme Validation Report, Apple iPad and iPhone Mobile Devices with iOS 12, Report Number CCEVS-VR-10937-2019, dated March 14, 2019, Version 0.2.

Documentation reported as being updated:

- Security Target – Apple iPad and iPhone Mobile Devices with iOS 12 Security Target, PP_MD_V3.1 with EP_MDM_AGENT_V3.0, PPWLAN_CLI_EP_V1.0, MOD_VPN_CLI_V2.1 Version 1.6, 2019-03-12, which has been updated to: Apple iPad and iPhone Mobile Devices with iOS 12 Security Target, PP_MD_V3.1 with

EP_MDM_AGENT_V3.0, PPWLAN_CLI_EP_V1.0, MOD_VPN_CLI_V2.1 Version 2.0, 2019-03-25.

- Apple iPad and iPhone Mobile Devices with iOS 12 Common Criteria Configuration Guide, PP_MD_V3.1 with EP_MDM_AGENT_V3.0, PPWLAN_CLI_EP_V1.0, MOD_VPN_CLI_V2.1, Version 1.7, 2019-03-12, which has been updated to Apple iPad and iPhone Mobile Devices with iOS 12 Common Criteria Configuration Guide, PP_MD_V3.1 with EP_MDM_AGENT_V3.0, PPWLAN_CLI_EP_V1.0, MOD_VPN_CLI_V2.1, Version 2.0, 2019-04-15

Assurance Continuity Maintenance Report:

On behalf of Apple Inc., atsec information security Corporation submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 18 April 2019. 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.

The purpose of this ACMR is to summarize and present CCEVS' analysis and findings regarding Assurance Maintenance Continuity for the addition of new mobile device hardware and minor maintenance software updates to the evaluation.

Introduction:

VID10937, Apple Inc. iPad and iPhone Devices with iOS12 was evaluated by atsec information security corporation for Apple Inc. The product met the requirements specified by the NIAP-approved protection profile, extended packages and module:

- Mobile Device Fundamentals Protection Profile, Version 3.1, dated 16 June 2017;
- Extended Package for Mobile Device Management Agents, Version 3.0, dated 21 November 2016;
- General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package Wireless Local Area Network {WLAN} Clients, Version 1.0, dated 8 February 2016 and,
- The PP-Module for Virtual Private Network {VPN} Clients, Version 2.1, dated 5 October 2017

Summary Description:

The vendor has made software changes to address bug fixes and added new features to the software along with the addition of eight Apple iPad mobile devices that were not released in time to be included in the 10937 evaluation. The CC Configuration Guide and the Security Target have been updated to reflect the additional hardware and software.

Changes to TOE:

The changes are divided into three categories: the addition of New Features, New Hardware and Security Fixes. The subsections below justify that changes have no security relevance on the certified TOE.
Only changes to the ST and the Administrative Guide are required to add a new device model to the list of device models supported by this evaluation because said device model contains the same A12 Bionic processor and runs the same (or subsequent minor update release) version of iOS 12 as the A12 Bionic device models which were originally included in the evaluation.

New Features:

iOS has had two minor updates beyond those considered in VID10937: iOS 12.1.4 and iOS 12.2. Such updates are a regular occurrence for iOS.

- iOS 12.1.4 did not include new non-security features.

Details on the iOA 12.1.4 security related fixes can be found at: https://support.apple.com/en-us/HT209520 and are further detailed below in section "Security Fixes".

- iOS 12.2 included new non-security features.

Details about the non-security related features for iOS 12.2 can be found at: https://support.apple.com/guide/ipad/whats-new-in-ios-12-ipad8d9d296d/ios

The iOS 12.2 updates include:

- **Apple TV**
- **AirPlay 2 and smart TVs** support
- **Apple Pencil and Smart Keyboard** Support for earlier iPad models
- **Apple News+** subscription service
- **Group FaceTime** support
- **Animoji and Memoji** additions
- **Apple Music** updates
- **Messages** updates, such as filters and stickers
- **Screen Time Activity** reports – settings for time limits on iPhone and iPad use
- **Do Not Disturb** options setting for time or actions
- **Measure,** an application to get dimensions of real world objects via iPad camera.
- **Camera** updates
- **Photo** application updates
- **Siri** shortcuts
- **Voice Memo** updates
- **Battery Usage** updates
- **Stock** application updates

The new features have been reviewed to ensure they are correctly categorized as non-security functions. These changes do not affect any test Assurance Activities of the PP, EPs, or PP Module claimed in VID10937.

New Hardware Components:

Eight additional iPad devices were added to the evaluation. The 7.9-inch iPad mini 5th gen (models A2133, A2124, A2126, and A2125) and the 10.5-inch iPad Air 3rd gen (models A2152, A2123, A2153, and A2154) were released on March 18, 2019, four days after the TOE was validated. Therefore, they could not be included in the original evaluation.

These device models run the latest version of iOS 12 and contain the A12 Bionic processor. This is the same processor used by the iPhone XS, iPhone XS Max, and iPhone XR, which were included in the evaluation. As per the hardware equivalency argument used in VID10937 (as well as in VID10851, VID10782, VID10725, and VID10695), one device from each device / processor family was tested. Devices within the same device family were deemed equivalent for testing purposes, so any testing on one member of a device family applies to all devices within that device family.

The operational environment under which the validated cryptographic algorithm implementation was tested is the same as the operational environment as the changed TOE.

New Wi-Fi Alliance (WFA) certificates have been provided for the new device models as per the table below:

Processor	Device Name	Model Number	WFA Certificate
A12 BIONIC	**7.9-inch iPad mini**	**A2125**	**WFA 81121 / WFA81123**
		A2133	**WFA 81121 / WFA81123**
		A2124	**WFA 81121 / WFA81123**
		A2126	**WFA 81121 / WFA81123**
	10.5-inch iPad Air	**A2152**	**WFA 81122 / WFA81124**
		A2154	**WFA 81122 / WFA81124**
		A2123	**WFA 81122 / WFA81124**
		A2153	**WFA 81122 / WFA81124**

Security Fixes:

The updates to iOS 12.1.4 and iOS 12.2 included security relevant fixes for documented CVEs. The CVE databases were searched again on 4.15.2019 to ensure known security vulnerabilities have been corrected.

None of the security fixes resulted in changes to the evaluated security functionality of the devices, were below the level of detail of the SFR's and would not have affected assurance activity results.

iOS 12.1.4 – released February 7, 2019.

Vulnerability ID	Description	Impact	Mitigation
CVE-2019-6223	FaceTime issue	The initiator of a Group FaceTime call may be able to cause the recipient to answer.	A logic issue existed in the handling of Group FaceTime calls. The issue was addressed with improved state management.
CVE-2019-7286	Foundation issue	An application may be able to gain elevated privileges.	A memory corruption issue was addressed with improved input validation.
CVE-2019-7287	IOKit issue	An application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved input validation.
CVE-2019-7288	Live Photos in FaceTime issue	A thorough security audit of the FaceTime service uncovered an issue with Live Photos.	The issue was addressed with improved validation on the FaceTime server.

iOS 12.2 - released March 25, 2019

Vulnerability ID	Description	Impact	Mitigation
CVE-2019-8516	CFString issue	Processing a maliciously crafted string may lead to a denial of service.	A validation issue was addressed with improved logic.
CVE-2019-8552	configd issue	A malicious application may be able to elevate privileges.	A memory initialization issue was addressed with improved memory handling.
CVE-2019-8511	Contacts issue	A malicious application may be able to elevate privileges.	A buffer overflow issue was addressed with improved memory handling.

CVE-2019-8542	CoreCrypto issue	A malicious application may be able to elevate privileges.	A buffer overflow was addressed with improved bounds checking.
CVE-2019-8512	Exchange ActiveSync issue	A user may authorize an enterprise administrator to remotely wipe their device without appropriate disclosure.	This issue was addressed with improved transparency.
CVE-2019-8550	FaceTime issue	A user's video may not be paused in a FaceTime call if they exit the FaceTime app while the call is ringing.	An issue existed in the pausing of FaceTime video. The issue was resolved with improved logic.
CVE-2019-8565	Feedback Assistant issue	A malicious application may be able to gain root privileges.	A race condition was addressed with additional validation.
CVE-2019-8521	Feedback Assistant issue	A malicious application may be able to overwrite arbitrary files.	This issue was addressed with improved checks.
CVE-2019-6237	file issue	Processing a maliciously crafted file might disclose user information.	An out-of-bounds read was addressed with improved bounds checking.
CVE-2019-8553	GeoServices issue	Clicking a malicious SMS link may lead to arbitrary code execution.	A memory corruption issue was addressed with improved validation.
CVE-2019-8542	iAP issue	A malicious application may be able to elevate privileges.	A buffer overflow was addressed with improved bounds checking.
CVE-2019-8545	IOHIDFamily issue	A local user may be able to cause unexpected system termination or read kernel memory.	A memory corruption issue was addressed with improved state management.
CVE-2019-8504	IOKit issue	A local user may be able to read kernel memory.	A memory initialization issue was addressed with improved memory handling.
CVE-2019-8529	IOKit SCSI issue	An application may be able to execute arbitrary code with kernel privileges.	A memory corruption issue was addressed with improved input validation.
CVE-2019-8527	Kernel issue	A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.	A buffer overflow was addressed with improved size validation.
CVE-2019-8514	Kernel issue	An application may be able to gain elevated privileges.	A logic issue was addressed with improved state management.

CVE-2019-8540	Kernel issue	A malicious application may be able to determine kernel memory layout.	A memory initialization issue was addressed with improved memory handling.
CVE-2019-7293	Kernel issue	A local user may be able to read kernel memory.	A memory corruption issue was addressed with improved memory handling.
CVE-2019-6207 CVE-2019-8510	Kernel issue	A malicious application may be able to determine kernel memory layout.	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation.
CVE-2019-7284	Mail issue	Processing a maliciously crafted mail message may lead to S/MIME signature spoofing.	This issue was addressed with improved checks.
CVE-2019-8546	Messages issue	A local user may be able to view sensitive user information.	An access issue was addressed with additional sandbox restrictions.
CVE-2019-8549	Power Management issue	A malicious application may be able to execute arbitrary code with system privileges.	Multiple input validation issues existed in MIG generated code. These issues were addressed with improved validation.
CVE-2019-8541	Privacy issue	A malicious app may be able to track users between installs.	A privacy issue existed in motion sensor calibration. This issue was addressed with improved motion sensor processing.
CVE-2019-8566	ReplayKit issue	A malicious application may be able to access the microphone without indication to the user.	An API issue existed in the handling of microphone data. This issue was addressed with improved validation.
CVE-2019-8554	Safari issue	A website may be able to access sensor information without user consent.	A permissions issue existed in the handling of motion and orientation data. This issue was addressed with improved restrictions.
CVE-2019-6204 CVE-2019-8505	Safari Reader issue	Enabling the Safari Reader feature on a maliciously crafted webpage may lead to universal cross site scripting.	A logic issue was addressed with improved validation.

CVE-2019-8502	Siri issue	A malicious application may be able to initiate a Dictation request without user authorization.	An API issue existed in the handling of dictation requests. This issue was addressed with improved validation.
CVE-2019-8517	TrueTypeScaler issue	Processing a maliciously crafted font may result in the disclosure of process memory.	An out-of-bounds read was addressed with improved bounds checking.
CVE-2019-8551	WebKit issue	Processing maliciously crafted web content may lead to universal cross site scripting.	A logic issue was addressed with improved validation.
CVE-2019-8535	WebKit issue	Processing maliciously crafted web content may lead to arbitrary code execution.	A memory corruption issue was addressed with improved state management.
CVE-2019-6201 CVE-2019-8518 CVE-2019-8523 CVE-2019-8524 CVE-2019-8558 CVE-2019-8559 CVE-2019-8563	WebKit issue	Processing maliciously crafted web content may lead to arbitrary code execution.	Multiple memory corruption issues were addressed with improved memory handling.
CVE-2019-8562	WebKit issue	A sandboxed process may be able to circumvent sandbox restrictions.	A memory corruption issue was addressed with improved validation.
CVE-2019-6222	WebKit issue	A website may be able to access the microphone without the microphone use indicator being shown.	A consistency issue was addressed with improved state handling.
CVE-2019-8515	WebKit issue	Processing maliciously crafted web content may disclose sensitive user information.	A cross-origin issue existed with the fetch API. This was addressed with improved input validation.
CVE-2019-8536 CVE-2019-8544	WebKit issue	Processing maliciously crafted web content may lead to arbitrary code execution.	A memory corruption issue was addressed with improved memory handling.
CVE-2019-7285 CVE-2019-8556	WebKit issue	Processing maliciously crafted web content may lead to arbitrary code execution.	A use after free issue was addressed with improved memory management.
CVE-2019-8506	WebKit issue	Processing maliciously crafted web content may lead to arbitrary code execution.	A type confusion issue was addressed with improved memory handling.

CVE-2019-8503	WebKit issue	A malicious website may be able to execute scripts in the context of another website.	A logic issue was addressed with improved validation.
CVE-2019-7292	WebKit issue	Processing maliciously crafted web content may result in the disclosure of process memory.	A validation issue was addressed with improved logic.
CVE-2019-8567	Wi-Fi issue	A device may be passively tracked by its WiFi MAC address.	A user privacy issue was addressed by removing the broadcast MAC address.
CVE-2019-8530	XPC issue	A malicious application may be able to overwrite arbitrary files.	This issue was addressed with improved checks.

Affected Developer Evidence:

Modifications were made to the ST and Administrative Guide documents to add the eight new devices to the list of devices covered by the evaluation. Modifications were also made to the ST to list the WFA certificates for the eight new devices. No other developer evidence for VID10937 was affected.

Regression Testing:

The vendor performed regression testing to ensure correct operation of the updated software as a matter of course for each minor release. Each individual change was unit tested; furthermore, the changes covered by the IAR do not relate to any SFR/SAR evaluated in VID10937.

In addition, the developer confirmed the changed TOE conforms to NIAP Policy 5. The operational environment under which the validated cryptographic algorithm implementation was tested is the same as the operational environment as the changed TOE. Therefore, the cryptographic algorithm implementation validated for CAVP conformance also applies to the changed TOE.

Vulnerability Analysis:

Since the evaluation was completed, several minor updates of Apple iOS have been released as normal maintenance updates to the Apple 11.2 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.

To confirm no other publicly known vulnerabilities exist apart from those summarized above, a new CVE search was performed on 2019-04-15 using the same search terms and web sites used in the search performed for AVA_VAN.1 in VID10937.
The sites used for the searches were:

- MITRE Common Vulnerabilities and Exposures (CVE) list, http://cve.mitre.org/cve/search_cve_list.html

- NIST National Vulnerability Database (NVD), https://nvd.nist.gov/vuln/search

The search terms used were:

- ios ipad
- ios iphone
- ios core tls
- ios core crypto
- ios common crypto
- ios http
- ios https
- ios tcp
- ios ip
- ios bluetooth
- ios ipsec
- ios vpn
- ios mdm
- ios mobile
- broadcom wi-fi

No new vulnerabilities were found apart from those which have been mitigated in the subsequent releases.

Conclusion:

CCEVS reviewed the vendor provided description of the analysis of the devices and found there to be only minor impact upon security related functionality, below the level of detail of the SFRs, and would not have changed assurance activity results. 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.