ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
Cisco AnyConnect Secure Mobility Client for Apple iOS 11.2

Maintenance Update for: Cisco AnyConnect Secure Mobility Client for Apple iOS 11.2

Maintenance Report Number: CCEVS-VR-VID10880-2019

Date of Activity: 11 February 2019

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- Cisco AnyConnect for Apple iOS Impact Analysis Report, Update of Cisco AnyConnect Secure Mobility Client v4.6 for Apple iOS 11.2 To Cisco AnyConnect Secure Mobility Client v4.7 for Apple iOS 11.2 (IAR), Version 0.1, February 11, 2018
- Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, dated 12 October 2013 [VPNv1.4]
- Validation Report for Cisco AnyConnect Secure Mobility Client v4.6 for Apple iOS 11.2, Report Number CCEVS-VR-10880-2018, dated June 4th, 2018, Version 0.3.

Documentation reported as being updated:

- Security Target – Cisco AnyConnect Secure Mobility Client for Apple iOS 11.2 (Updated to Version 0.6, 11 Feb 2019)

- Common Criteria Guide - Cisco AnyConnect Secure Mobility Client for Apple iOS 11.2 CC Configuration Guide (Updated to Version 0.5, February 2019)

Assurance Continuity Maintenance Report:

Cisco Systems Inc, submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 11 February 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.

CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

Introduction:

VID10880, Cisco AnyConnect Secure Mobility Client for Apple iOS 11.2 was evaluated by Gossamer Security Solutions for Cisco Systems Inc, 2018-06-08. The product met the requirements specified by the NIAP-approved protection profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, dated 12 October 2013 [VPNv1.4]

The purpose of this document is to summarize and present CCEVS' analysis and findings regarding Assurance Maintenance Continuity as the Secure Mobility Client is upgraded from v4.6 to v4.7. The approved mobile platform covered by VID10880 and subsequent Assurance Continuity is the Apple iPhone 7/7Plus running iOS 11.2.

Summary Description:

The vendor has made software changes to address bug fixes and add new features to version 4.7 of the software. The CC Configuration Guide and the Security Target have been updated to reflect the new version of software.

Changes to TOE:

The changes are divided into two categories: new features and bugfixes. The subsections below justify that changes to version 4.7 have no security relevance on the certified TOE.

New Features: The following table lists and describes each feature and provides supporting rationale regarding security relevance.

Feature	Analysis and Supporting Rationale
Managing NSUserDefault for External Control usage	NSUserDefault is platform provided programmatic interface used to persist small amounts of data between launches of an application, for example, sound settings and preferred screen orientations. This does not apply to any security credentials. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
Sharing AnyConnect logs via iOS Share Extension	This new feature does not directly correlate to a TOE Security function in the Security Target. However, since log file may contain TSF data, a warning was added to AGD section 4.6 to not share AnyConnect app log files outside of the protection provided by the mobile platform.
Support for SAML authentication	SAML authentication does not apply to the IPsec VPN client. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
VPN TLS ECDSA client certificate support	New support for TLS ECDSA client certificate is only applicable to SSL VPN. The VPN Client permits only IPsec VPN. Therefore, support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
Support for DTLSv1.2	New support for DTLS 1.2 is only applicable to SSL VPN. The VPN Client permits only IPsec VPN. Therefore, support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.

Bug Fixes The fixes listed in the table below do not directly apply to the TSF or fell out of the scope of evaluated functionality.

Identifier	Description of the Issue	Analysis and Supporting Rationale
CSCvn30076	AC Network Extension logs not always retrieved	The Network Extension logs are outside of the TOE evaluated configuration. In addition, the bug fix corrects a specific situation where those logs are not accessible which is only when the extension is launched via On Demand or Per-App. This also does not apply to the TOE. Therefore, this bug fix does not impact TOE security functions.
CSCvm94880	No biometric prompt when TouchID enabled for certificate. User should get TouchID or FaceID prompt when certificate is protected, and finger or face is enrolled.	This issue applies to iOS 12. It is not an issue for iOS 11.2, which is the mobile platform the AnyConnect TOE was certified on. Therefore, this bug fix does not impact TOE security functions.
CSCvn00655	AnyConnect app doesn't rotate on the new iPhone devices (XS/XR/XS Max).	App orientation does not have a security impact to the TOE. In addition, iPhone XS/SR/XS Max are not the devices the AnyConnect TOE was certified on. Therefore, this bug fix does not impact TOE security functions.
CSCvb78548	VPN Fails to transition from Wi-Fi to Cellular using T-Mobile IPv6 Network.	This issue is only applicable to SSL VPN. The VPN Client permits only IPsec VPN. Therefore, this bug fix does not impact TOE security functions.
CSCvi79881	AC Apple iOS stuck in Examining System when roaming between IPv4 only <-> IPv6 only network	This issue is only applicable to SSL VPN. The VPN Client permits only IPsec VPN. Therefore, this bug fix does not impact TOE security functions.
CSCvm96366	Installing per-app VPN using MDM to push the profile. Users see a one-time pop-up	This per app VPN issue applies only to SSL VPN. This issue does not apply to IPsec, which the VPN Client PP requires. Therefore, this bug fix does not impact TOE security functions.
CSCvm12157	SVC Message: 17/ERROR: Reconnecting to recover from error.	The message falsely indicated an 'Error' when in fact there was not. In addition, this issue is only applicable to SSL VPN. The VPN Client permits only IPsec VPN. Therefore, this bug fix does not impact TOE security functions.

Affected Developer Evidence:
None

Regression Testing:

The vendor performed regression testing to ensure correct operation of the updated software as a matter of course. Each individual change was unit tested, and the 4.7 software image has had a limited amount of automated regression testing covering all major areas of baseline client functionality. This regression testing was conducted on both the evaluated Apple iOS 11.2 version, and on subsequent versions of Apple iOS.

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 for the changed TOE. Therefore, the cryptographic algorithm implementation validated for CAVP conformance also applies to the changed TOE.

Vulnerability Analysis:

A search of the following national sites was conducted for vulnerabilities related to the Cisco AnyConnect 4.7 TOE. There were no vulnerabilities found for AnyConnect v4.7 iOS.

- National Vulnerability Database: https://nvd.nist.gov
- US-CERT: https://www.us-cert.gov
- Security Focus: www.securityfocus.com

The following key words, product, and vendor were each selected for search criteria:

Product:

- AnyConnect Secure Mobility Client for iOS

Vendor:

- Cisco

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

Conclusion:

CCEVS reviewed the vendor provided description of the analysis of the devices and found there to be no impact upon security-related functionality as defined in the ST. Therefore, under Scheme Publication 6, this is classified as a minor update. 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 on both the original, evaluated version of the iOS platform, and on subsequent versions of iOS. Therefore, CCEVS agrees that the original assurance is maintained for the product.