CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Cisco Secure Client - AnyConnect 5.1 for Windows 10

Maintenance Report Number: CCEVS-VR-VID11398-2024

Date of Activity: September 24, 2024

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." 29 August 2014.

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

Cisco Secure Client - AnyConnect 5.0 for Windows 10 Impact Analysis Report For Common Criteria Assurance Maintenance, Version 0.2, September 24, 2024

Cisco Secure Client - AnyConnect 5.1 for Windows 10 Security Target, Version 0.7, August 20, 2024

Cisco Secure Client - AnyConnect 5.1 for Windows 10 CC Configuration Guide, Version 0.3, August 20, 2024

Assurance Continuity Maintenance Report:

Cisco Systems, Inc. submitted an Impact Analysis Report (IAR) for the changes from the certified TOE, Cisco Secure Client - AnyConnect 5.0 for Windows 10 to Cisco Secure Client - AnyConnect 5.1 for Windows 10, to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on August 22, 2024. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Reevaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the Security Target (ST), the Administrator's Guide (AGD), and the Impact Analysis Report (IAR).

The ST and AGD were updated to reflect the new version of the TOE.

- The new features did not change how the TSF performed, and the TOE continues to implement the TSF in a manner that is consistent what is defined in the Security Target.
- The bug fixes did not change how the TSF performed, and the TOE continues to implement the TSF in a manner that is consistent what is defined in the Security Target. There were no negative impacts due to bug fixes and no documentation needed to be updated.
- There was no change to the operational environment for the evaluated configuration of the TOE. Therefore, the TOE environment for Cisco Secure Client - AnyConnect 5.1 for Windows 10 presents no impact to the overall evaluation.

Documentation Updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Cisco Secure Client - AnyConnect 5.0 for Windows 10 Security Target, Version 0.4, December 6, 2023	Cisco Secure Client - AnyConnect 5.1 for Windows 10 Security Target, Version 0.5, August 20, 2024 Updated to reflect updated version 5.1 software version number.
Design Documentation: See Security Target and Guidance	Updated ST and AGD to reflect updated version 5.1 software version number.
Guidance Documentation: Cisco Secure Client - AnyConnect 5.0 for Windows 10 CC Configuration Guide, Version 0.3, December 6, 2023	Cisco Secure Client - AnyConnect 5.1 for Windows 10 CC Configuration Guide, Version 0.4, August 20, 2024 Updated to reflect updated version 5.1 software version number.
Lifecycle: NONE	No changes required
Testing: NONE	See Description of Regression Testing section.
Vulnerability Assessment: NONE	The public search was updated on September 24, 2024. No public vulnerabilities exist within the product. See analysis of results below.

Changes to TOE:

The TOE has been updated from Cisco Secure Client - AnyConnect 5.0 for Windows 10 to AnyConnect 5.1 for Windows 10. The changes are divided into two categories: New Features/Support Updates and Bug Fixes. New features in the product were analyzed and determined to have no security relevance or fell out of the scope of evaluated functionality. All CVEs and Bug Fixes are either not applicable or mitigated in the updated TOE version 5.1. Below is a summary of the changes.

Major Changes: None

Minor Changes:

Eight new features/support updates and forty-five bug fixes were identified in the IAR between versions 5.0 and 5.1 along with a description and given rationale. The description and rationale for each bug fix or enhancement was inspected, and the overall Minor Change characterization was considered appropriate. None of the changes resulted in the introduction of new TOE capabilities, modification to security functions as defined in the ST, or changes to the TOE boundary. The following table includes a summary of the changes presented in the IAR that impact one or more of the evaluated platforms. The changes have been categorized according to New Features and Bug Fixes.

Category	Number of Changes	Assessment
New Features/Support Updates	8	• 2 updates are related to user preferences • 2 updates are related to performance enhancement • 1 update is related to accessibility improvements • 1 update is related to GUI enhancement • 1 update is related to unsupported processor • 1 update is related to OS deployment options
Bug Fixes	45	45 – Bug Fixes were made for issues identified in previous releases. The bug fixes break out into the following categories: 25 – Correct expected behavior and has no direct impact to the secure operation/functionality of the TOE 20 - Outside the Scope of TOE None of the bug fixes affected the security functionality required by the SFRs and none of the changes resulted in changes to the ST or guidance documentation. As noted, these changes were either unrelated to SFRs or outside the scope of the TOE. Thus, the original testing still holds, and any fix testing was covered by vendor non-evaluation regression testing.

Description of Regression Testing:

During development of a new version of Cisco Secure Client – AnyConnect for Windows, there are various tests performed to ensure the product performs as expected. Bug fixes and new features are tested to ensure the feature works as expected or the fix was effective. Additionally, regression testing, using pre-defined test cases, is performed to ensure that overall product performs as expected, in essence ensuring existing features and functionality from previous versions was not broken in the development of the latest version.

Based on the bug fix and regression testing, Cisco believes the product behaves as expected.

NIST CAVP Certificates:

Specific to NIAP Policy No. 5, the version of the CiscoSSL FIPS Object Module (FOM) Cryptographic Implementation remains the same, which is 7.2a. The CAVP certificate to SFR mappings in Table 16 of the ST are unchanged and remain valid in version 5.1 of Cisco Secure Client for Windows 10.

Vulnerability Assessment:

The IAR contains the output from the vulnerability searches since the time of the original evaluation search (December 11, 2023) to September 24, 2024, as well as the rationale why the vulnerabilities identified in the search results are not applicable to the TOE.

The same vulnerability databases and search teams listed in the assurance activities were used:

- National Vulnerability Database: (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative(http://www.zerodayinitiative.com/advisories)
- cve.org CVE Database (https://www.cve.org/)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The search terms used were:

- "anyconnect 5.1"
- "cisco anyconnect ikev2"
- "cisco anyconnect encapsulating security payload"
- "cisco anyconnect"
- "anyconnect windows 10"
- "rapidxml"
- "boost"
- "libcurl"
- "ciscossl"
- "cisco fom"

- "zlib"
- "intel core i5-1135g7"

The vulnerability search returned thirty results. The results of the vulnerability assessment were included in the IAR. No new vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

New features in the product were analyzed and determined to have no security relevance or fell out of the scope of evaluated functionality.

Bug fixes are tracked within Cisco's distributed defect tracking system (DDTS). Each bug, whether identified by a customer or within Cisco is tracked within DDTS and given a DDTS identifier.

Each DDTS report contains a brief "headline" and more detailed discussion of the problem and the resolution. The vendor examined each of the detailed DDTS reports and drafted the "brief description" found in the tables below by referencing the DDTS headline and the report details. The vendor made the determination of which category was applicable for each report by examining the "headline" and classifying those that involved items into category. Each of the software fixes fell into the following categorization:

- Minor Changes with No Security Relevance: These changes may indirectly be related to the TSF in some way, though were not directly related to an SFR defined in the claimed Protection Profiles and the Security Target.

None of the software fixes fall into this category:

- Major Changes: These changes can be directly related to some SFR and modify how the TOE meets that SFR such that the TSS or design documents are no longer accurate.

Validation Team Conclusion:

The validation team reviewed the changes, and concur that the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The updates described above were made to support the new TOE version number.

Regression testing was done and was considered adequate based on the scale and types of changes made. The vendor also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. In addition, the platforms did not change and there were no necessary alterations to the NIST cryptographic certificates. Therefore, CCEVS agrees that the original assurance is maintained for the product.