ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Cisco Network Convergence System 1000 Series (NCS1000)

Cisco Network Convergence System 1000 Series (NCS1000)

Maintenance Report Number: CCEVS-VR-VID11093-2020

Date of Activity: 9 September 2020

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Cisco Network Convergence System 1000 Series Impact Analysis Report, Version 1.1, 1 September 2020
- NDcPP - collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018

Assurance Continuity Maintenance Report:

Gossamer submitted an Impact Analysis Report (IAR) for the Cisco Network Convergence System 1000 Series to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 1 September 2020. 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 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 Operational User Guide, and the Impact Analysis Report (IAR). The ST, User Guide, and the IAR were all updated.

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: Cisco Network Convergence System 1000 Series (NCS1000) Security Target, Version 1.0, July 7 2020	The ST was updated to reflect IOS-XR software version 7.2

Guidance: Cisco Network Convergence System 1000 Series Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0, July 7 2020	The CC Configuration Guide was updated to reflect IOS-XR software version 7.2.1.

Changes to the TOE:

Each of the software fixes to Cisco Network Convergence System 1000 Series fell into the following categorization:

Major Changes

None.

Minor Changes

Software bug fixes resulted in what were considered to be "Minor Changes". There were 12 bug fixes implemented in all, between IOS-XR version 7.0 and 7.2.1. The rational in the IAR for each was inspected and the overall Minor Change characterization was considered appropriate. Changes related to the Optical Service Channel; pluggable registration; FPD downgrade; Reload errors; Install Commit log message failures and re-applying the Network Terminal Loopback; No functionality, as defined in the SFRs, was impacted, and none of the software updates affected the security functionality or the SFRs identified in the Security Target.

Regression Testing:

Each individual change was unit tested, and the IOS-XR 7.2.1 software image has had a limited amount of automated regression testing covering all major areas of baseline client functionality. Testing was completed by Cisco Business Unit engineers and developers. There were no changes to any SFR or SAR therefore detailed regression testing was not required.

NIST CAVP Certificates:

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:

A public search for vulnerabilities that might affect the TOE was performed on August 17, 2020. All vulnerabilities found using the national sites and search terms below have been addressed in the release of IOS-XR 7.2.1 (version of the TOE under Assurance Maintenance).

A search of the following national sites was conducted:

- 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:

- Cisco Network Convergence System 1000 Series (NCS 1001)
- Cisco Network Convergence System 1000 Series (BCS 1004)
- IOS-XR
- Cisco IOS-XR 7.2
- Intel Atom C2516
- Intel Atom C3758
- Cisco FIPS Object Module 6.0

Vendor:

- Cisco

Summary of the analysis

The vulnerability search returned 15 results. Most issues were protocol and code vulnerabilities discovered in the IOS XR software that were mitigated in version 7.2.1. Other vulnerabilities discovered did not directly impact the TOE or were not relevant to the evaluated configuration.

Conclusion:

The overall impact is minor. This is based on the above rationale that bug fixes to update the IOS-XR version to 7.2.1 have no Security Relevance on the certified TOE.

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