CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec running ArubaOS-CX version 10.13

Maintenance Report Number: CCEVS-VR-VID11422-2024

Date of Activity: May 28, 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

Collaborative Protection Profile for Network Devices Version 2.2e, 23 March 2020 [NDcPP]

PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 [MACSEC]

Impact Analysis Report for HPE Aruba Networking HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec, Version 0.3, May 28, 2024

HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec Security Target, version 1.2, May 28, 2024

HPE Aruba Networking Common Criteria Administrator Guide Target of Evaluation: Aruba 6300M and 8360v2 Switch Series, Version 2.6, May 10, 2024

Assurance Continuity Maintenance Report:

Aruba, a Hewlett Packard Enterprise Company, currently branded as HPE Aruba Networking, submitted an Impact Analysis Report (IAR) for the HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec running ArubaOS-CX version 10.13 (was Version 10.11) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on April 29, 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, and the Impact Analysis Report (IAR). The ST and Admin Guide were updated to reflect the new version of the TOE and updated vendor branding.

- 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 HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec running ArubaOS-CX version 10.13 presents no impact to the overall evaluation.

Documentation Updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Aruba, A Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec Security Target, Version 1.0, April 10, 2024	See references above. Document is updated to reflect the new version number. References to "Aruba, A Hewlett Packard Enterprises Company" are now updated to say "HPE Aruba Networking" consistent with new branding. Section 1.4.2 was updated to provide the correct current name and version of the AGD. The version of the ST is now 1.2 and the date May 28, 2024
Design Documentation: See Security Target and Guidance	No changes have been made to the Security Target or Guidance documentation beyond revisions to identify the new version of the TOE.
Guidance Documentation: HPE Aruba Networking Common Criteria Administrator Guide Target of Evaluation: Aruba 6300M and 8360v2 Switch Series, Version 2.5, April 4, 2024	See references above. Document is updated to reflect the new version number. Aruba, A Hewlett Packard Enterprises Company" are now updated to say "HPE Aruba Networking" consistent with new branding. The version is now 2.6 and the date is updated to May 10, 2024. Appendix B has been updated with current instructions on accessing the HPE Aruba

	Networking support portal to find additional documentation and release notes. These release notes can also be found at the link below: Networking Support
Lifecycle: None	No changes required
Testing: None	HPE Aruba Networking has performed regression testing on the evaluated product. The dedicated quality assurance team for the CX switching team performs testing on all new features and bug fixes, as well as regression testing against existing features prior to releasing a new version. This testing is consistent with recognized best practices in quality assurance.
Vulnerability Assessment: None	The public search was updated on May 28, 2024. No public vulnerabilities exist within the product. See analysis of results below.

Changes to TOE:

The TOE has been updated from HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec running ArubaOS-CX version 10.11 to version 10.13. Below is a summary of the changes.

Major Changes

None.

Minor Changes

Thirty enhancements and forty-four bug fixes were identified in the IAR between versions 10.11 and 10.13 along with a description and given rationale. Not all changes impacted all hardware platforms. 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 Enhancements and Bug Fixes.

Category	Number of Changes	Assessment
Enhancements	30	30 Enhancements were made that impacted the management, control, or security of data plane traffic, the boot process, NTP, SNMP, and Access Point deployments, which are not covered by the SFR functionality claimed. Specifically, 2 of the 30 Enhancements updated functionality related to commands and logging, but did not impact the evaluated configuration: • 1 provides a new command structure, but the structure covered in the AGD is still functional and preferred. • 1 provides additional information in the logs that is not required by the PP
Bug Fixes	44	44 Bug Fixes were made for issues identified in previous releases. The bug fixes break out into the following categories: 34 - Unrelated to SFRs 7 - Outside the Scope of the Evaluated Configuration 2 – Provides additional information not required by the PP or modifies the capture of information but does not impact what is required by the PP 1 – Resolved an unexpected process crash that

		was not impacting claims related to the SFR. 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, outside the scope of the evaluated configuration, or did not impact the ability to meet the requirements of the PP/SFRs. Thus, the original testing still holds, and any fix testing was covered by vendor non-evaluation regression testing.

Description of Regression Testing:

HPE Aruba Networking has performed regression testing on the evaluated product. The dedicated quality assurance team for the CX switching team performs testing on all new features and bug fixes, as well as regression testing against existing features prior to releasing a new version. This testing is consistent with recognized best practices in quality assurance.

Equivalency:

The security functionality of the 10.13 software update remains the same as the prior evaluated version. The hardware platforms are unchanged from the original evaluation version.

NIST CAVP Certificates:

The same cryptographic modules are used in 10.13 and in 10.11. The CAVP certificate numbers referenced during the 10.11 evaluation have not changed.

Vulnerability Analysis:

The IAR contains the output from the vulnerability searches since the time of the original evaluation search (dated April 3, 2024) to May 28, 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:

- ArubaOS
- AOS 10.11
- TLS
- SSH
- Cortex A9
- NPX 1046A
- Xeon D-1518
- Xeon D-1527
- Xeon D-1537
- Xeon D-1637
- Atom C2538
- AOS-CX
- AOS-CX RSA Engine
- AOS-CX Crypto
- AES ECB
- MACsec
- AOS 10.13
- AOS-CX 10.13

The vulnerability search returned 75 results. The results of the vulnerability assessment were included in the IAR. No new vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

The evaluation evidence consists of the Security Target and administrative guidance. The Security Target was revised to reflect the new software version of 10.13, as well as new corporate branding for the vendor.

Note that HPE Aruba Networking continually tracks bugs, vulnerabilities, and other defects reported in the public domain and that as of the time of this report there are no known outstanding security-related vulnerabilities in the TOE.

In review of all changes made within the evaluated TOE, the vendor has determined that the overall impact to the product in upgrading from 10.11 to 10.13 is minor. The changes made within the product

do not impact the requirements as claimed within the Security Target and allow for continued operation of the product in conformance with the protection profiles.

Validation Team Conclusion:

The overall impact is minor. This is based on the rationale that updates do not change any security policies of the TOE and are unrelated from SFR claims. The updates described above were made to support the new TOE minor 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.