ASSURANCE CONTINUITY MAINTENANCE REPORT FOR HPE Aruba Networking 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.13

HPE Aruba Networking 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.13

Maintenance Report Number: CCEVS-VR-VID11391-2024

Date of Activity: May 30, 2024

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Impact Analysis Report for HPE Aruba Networking 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series running ArubaOS-CX 10.13, Revision .4, 15 May 2024
- HPE Aruba Networking 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.13 Security Target, Version .8, May 8, 2024
- HPE Aruba Networking Common Criteria Administrator Guidance, Target of Evaluation: Aruba 4100, 6000, 8000, 9000, and 10000 Switch Series, Version 2.5, May 6, 2024
- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)

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 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.13 (was Version 10.11) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on May 15, 2024. 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 Administrator’s Guide, and the Impact Analysis Report (IAR). The ST and Admin Guide were updated to the new version of the TOE.

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary
Security Target: Aruba, A Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11 Security Target, Version 0.7, December 4, 2023	**Maintained Security Target:** See references above. Updated to identify the new TOE version number and updated AGD version and date. Updated references to “Aruba, A Hewlett Packard Enterprise Company” to indicate “HPE Aruba Networking” consistent with new branding.
Design Documentation: See Security Target and Guidance	No changes required
Guidance Documentation: HPE Aruba Networking Common Criteria Administrator Guidance, Target of Evaluation: Aruba 4100, 6000, 8000, 9000, and 10000 Switch Series, Version 2.4, November 28, 2023	**Maintained Guidance Documentation:** See references above. Revised to refer to the current product version and release notes for the current version.
Lifecycle: None	No changes required.
Testing: None	HPE Aruba Networking has performed regression testing on 10.13 on all platforms claimed in the evaluated configuration. This regression testing is conducted by a dedicated quality assurance team for HPE Aruba Networking’s switching team. The testing executed by the quality assurance team exercises all functionality of the product, including those claimed within the scope of the Common Criteria evaluations.
Vulnerability Assessment: None	The public search was updated on May 9, 2024. No public vulnerabilities exist in the product. See analysis results below.

Changes to the TOE:

The TOE has been updated from Aruba, A Hewlett Packard Enterprise Company 4100i, 6200, 6300, 6400, 8320, 8325, 8360, 8400, 9300, and 10000 Switch Series Version 10.11 to Version 10.13. Below is a summary of the changes.

Major Changes

None.

Minor Changes

Ninety-six bug fixes and thirty-four enhancements 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 Bug Fixes and Enhancements.

Category	Number of Changes	Assessment
Bug Fixes – version 10.11 to 10.12	35	34 Bug Fixes were made for issues identified in previous releases. The bug fixes break out into the following categories: 29 - Unrelated to SFRs 6 - Outside the Scope of the Evaluated Configuration None of the bug fixes affected the security functionality 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 evaluated configuration. Thus, the original testing still holds, and any fix testing was covered by vendor non-evaluation regression testing.
Bug Fixes – version 10.12 to 10.13	61	61 Bug Fixes were made for issues identified in previous releases. The bug fixes break out into the following categories: 53 - Unrelated to SFRs 5 - 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.
Enhancements – version 10.11 to 10.13 (no enhancements in 10.12)	34	34 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 34 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.

Regression Testing:
As noted above, HPE Aruba Networking has performed regression testing on 10.13 and all platforms in the ST have been subject to testing. This regression testing is conducted by the dedicated Quality Assurance team for HPE Aruba Networking’s switching. As part of all product releases, testing includes all functionality of the product, including testing in accordance with the Common Criteria requirements to ensure no previous functionality has been impacted.

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:
A new search was performed for vulnerabilities from the time of the original evaluation (November 29, 2023) to May 9, 2024. The search was conducted against the same vulnerability databases and

used the same terms as the original evaluation: "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" as well as “AOS 10.13” and “AOS-CX 10.13”.

The vulnerability search returned 72 results. The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were found.

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.