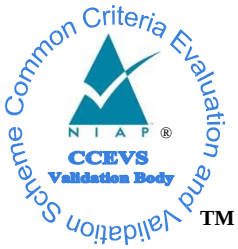

ASSURANCE CONTINUITY MAINTENANCE REPORT for Aruba, a Hewlett Packard Enterprise Company 8320 8325 and 8400 Switch Series

---

Maintenance Update for: 8320 and 8400 Switch Series running Aruba OS-CX version 10.01

Maintenance Report Number: CCEVS-VR-VID10919-2019b

Date of Activity: 16 October 2019

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- Impact Analysis Report for Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series (IAR), Version 1.2, July 26, 2019
- Collaborative Protection Profile for Network Devices, Version 2.1, dated 24 September 2018.
- Validation Report for Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series, Report Number CCEVS-VR-10919-2018, dated October 30, 2018, Version 0.3.

Documentation reported as being updated:

- Security Target – Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series (NDcPP20E) Security Target. Updated to: Aruba, a Hewlett Packard Enterprise Company 8320, 8325, and 8400 Switch Series (NDcPP20E) Security Target Version 0.6, 26 July 2019.
- Common Criteria Guide - Aruba, a Hewlett Packard Enterprise Company Common Criteria Admin Guide, Version 1.1, October 24, 2019. Updated to: Aruba, a Hewlett Packard Enterprise Company, Common Criteria Admin Guide, Version 1.4, June 26, 2019.
- ArubaOS-CX 10.03.001 Release Notes for the Aruba 8325 Switch Series, January 2019.
- ArubaOS-CX 10.03.001 Release Notes for the Aruba 8320 Switch Series, June 2019.
- ArubaOS-CX 10.03.001 Release Notes for the Aruba 8400 Switch Series, June 2019.

Assurance Continuity Maintenance Report:

The purpose of this document is to summarize and present CCEVS' analysis and findings regarding Assurance Maintenance Continuity as the Aruba Switch Series software is upgraded from v10.02 to 10.03.

Introduction:

Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series was evaluated by Gossamer Security Solutions on October 30, 2018. The product met the requirements specified by the NIAP-approved protection profile for Collaborative Protection Profile for Network Devices, Version 2.1, dated 24 September 2018.

Aruba, a Hewlett Packard Enterprise Company, submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 26 July 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.

Summary Description:

The vendor made software changes to add new features to version 10.03 of the software, and to fix bugs discovered in the previous version. The CC Configuration Guide and the Security Target have been updated to reflect the new version of software.

Changes to TOE:

The changes are related to new non-security features and bug fixes. The TOE has been revised from the evaluated ArubaOS-CX version 10.02 to version 10.03. The subsections below justify that changes to version 10.02 have no security relevance on the certified TOE.

The following table lists and describes each new feature and provides supporting rationale regarding security relevance.

New Feature Description	Assessment
BFD (Bidirectional Forwarding Detection) support added.	Network traffic detection is outside the scope of the NDcPP evaluation.
Added support for ingress global policy.	Policies on interfaces are outside the scope of the NDcPP evaluation.
CLI addition - Added support for interface range commands.	This is an extra set of commands not needed for the NDcPP evaluation.

DHCP server - Aruba 8000 series switches now offer both IPv4 and IPv6 DHCP Server services, each with a separate CLI context for ease of use.	Evaluating the TOE as an DHCP server was not part of the NDcPP evaluation.
Ethernet Ring Protection Switching – Ethernet Ring Protection Switching (ERPS) provides protection and recovery switching for Ethernet traffic in a ring topology, ensuring no loops are formed at the Ethernet layer.	Ring topology considerations are outside the scope of the NDcPP evaluation.
Loop Protect - Increased the total amount of loop protect instances from 4k to 10k.	Loop protection is outside the scope of the NDcPP evaluation.
Multicast Source Discovery Protocol (MSDP) allows multicast routes to be shared between PIM domains, preventing massive source/group trees.	MSDP functionality was not included in the evaluated configuration.
NTP - Added support for broadcast IP address for NTP server configuration.	Evaluating the TOE as an NTP server was not part of the NDcPP evaluation.
Network Analytics Engine (NAE) scripts can be upgraded without adding/removing the agent. This update also allows some parameters to be either optional or required.	NAE scripts are outside the scope of the NDcPP evaluation.
OSFP - Add support for Default Originate functionality.	Routing protocols are outside the scope of the NDcPP evaluation.
PIM-SM RP ACL enables securing which routers are allowed to become RPs in the network.	Routing protocols are outside the scope of the NDcPP evaluation.
Reverse Path Forwarding - New CLI commands to enable and disable Reverse Path Forwarding (RPF) were added.	Reverse Path Forwarding was not in the scope of the NDcPP evaluation.
VLAN translation allows remapping of VLANs during transit.	VLANs are outside the scope of the NDcPP evaluation.
VSX Features – • VSX interoperates with RPVST+ • VSX graceful upgrade for routing features enables automated traffic draining for the VSX member about to be • upgraded • VSX synchronization of global VSX configurations on the primary VSX node to the secondary peer • VSX synchronization of global STP configurations on the primary VSX node to the secondary peer	VSX is outside the scope of the NDcPP evaluation.

Bug Fixes:

The defects were primarily of a functional nature and none has any bearing on the security requirements in the evaluated ST.
The bug fixes are described in more detail in the switch family related Release Notes.

Affected Developer Evidence:

CC Evidence	Evidence Change Summary
Aruba, a Hewlett Packard Enterprise Company 8320 and 8400 Switch Series (NDcPP20E) Security Target, version 1.0, 01/16/2018	Updated to identify the new version number
Guidance Documentation: Aruba, a Hewlett Packard Enterprise Company Common Criteria Admin Guide, Version 1.3, March 26, 2019	Aruba, a Hewlett Packard Enterprise Company Common Criteria Admin Guide, Version 1.4, June 26, 2019. Release Notes updated to address version change.

Regression Testing:

Aruba performed regression testing of 10.03 on the switch platforms. All platforms in the ST have been subject to testing, and it was determined that the behavior of the TSF remained consistent with the original evaluation. This consistency confirms that the new features and bug fixes had no effect on any security-related functionality of the TOE.

Vulnerability Analysis:

A search of national sites was conducted for vulnerabilities related to the Aruba TOE. The public search was updated from 3/26/2019. No known vulnerabilities exist in the product.

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 an updated vulnerability search 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 Aruba platform, and on the subsequent versions of the TOE. Therefore, CCEVS agrees that the original assurance is maintained for the product.