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-VID10919-2019

Date of Activity: 5 April 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 1.1, March 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 0.5, 26 March 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 1.3, March 26, 2019.

Assurance Continuity Maintenance Report:

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

Introduction:

The 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.

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 v10.01 to v10.02 and an additional hardware switch series platform, the 8325, is added to the evaluation.

Summary Description:

The vendor has made software changes to add new features to version 10.02 of the software. The vendor has added the 8325 series of switches to the evaluation. The CC Configuration Guide and the Security Target have been updated to reflect the new version of software.

Changes to TOE:

The changes are divided into two categories: new features and new hardware. The TOE has been revised from the evaluated ArubaOS-CX version 10.01 to version 10.02.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 feature and provides supporting rationale regarding security relevance.

New Feature Description	**Assessment**
6in4 Tunnels - Support for tunneling IPv6 traffic in an IPv4 network	Tunneling of network traffic is outside the scope of the NDcPP. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
• BGP connections over GRE tunnels • IPv6 multicast routing • Multi-protocol BGP (IPv6 routing) • Multicast routing - Loopback for RP and BSR is now supported for both IPv4 and IPv6.	Routing features are outside the scope of the NDcPP evaluation. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.

• Policy Based Routing (PBR) - a flexible feature for creating various routing decisions based on additional information in the packets.	
Control plane ACLs - Control plane ACLs control access to the control plane	ACLs are outside the scope of the NDcPP evaluation. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
Egress queue shaping - limits the amount of traffic transmitted per output queue	Traffic limitations are outside the scope of the NDcPP evaluation. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
IPSLA – network monitoring	Network monitoring is outside the scope of the NDcPP evaluation. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
• Mirror to CPU - adds the capability to mirror dataplane packets to the CPU for monitoring directly on the switch using Tshark. • Remote mirroring - uses GRE encapsulated mirrored frames to a destination network device	Mirroring is outside the scope of the NDcPP evaluation. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
• NAE encrypted credentials - The Network Analytics Engine (NAE) now supports encrypted credentials for connecting to external services • NAE periodic callback actions - This feature introduces a new condition syntax to periodically execute a callback function for a given period of time. Using the Network Analytics Engine (NAE) python API, users can set callbacks to be called in regular intervals • NAE time series for external APIs- Using Network Analytics Engine (NAE) period callback actions, an NAE agent can be created using an	The NAE was not included in the evaluated configuration. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.

external API from another device or services.	
NTP master - allows the switch to act as the NTP master in the network	Evaluating the TOE as an NTP server was not part of the NDcPP evaluation. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
Object groups for ACLs - This feature enables the creation of named groups representing sets of IPv4 or IPv6 addresses and L4 port ranges. Object groups allow administrators to simplify their configurations	ACLs are outside the scope of the NDcPP evaluation. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
Rx Flow Control - Frames received on a port will pause sending egress packets. When the pause timer expires, the transmission of packets will proceed	Flow control is outside the scope of the NDcPP evaluation. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
Security- RADIUS accounting, PKI for syslog, and ServiceOS console password have been added to enhance security on the switch.	RADIUS and syslog PKI– these were not in the scope of the NDcPP evaluation. Service OS Password – this is the bootloader password. This is an added security feature but is not needed for the evaluation since the NDcPP assumes physical protection of the network device. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST .
Syslog over TLS - enables secure configuring of a syslog server with TLS security	TLS was not in the scope of the NDcPP evaluation. The syslog was protected with SSH in the evaluation. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
VLAN ACLs/Policies/Classifiers - ACLs, policies, and classifiers can now be applied to a VLAN interface.	VLANs are outside the scope of the NDcPP evaluation. Support for this feature does not impact the TOE security functions, and the functional capabilities of the features are not claimed as security functionality in the ST.
VSX Features – Expands spanning tree interoperability	VSX is outside the scope of the NDcPP evaluation. Support for this feature does not impact the TOE security functions, and the

	functional capabilities of the features are not claimed as security functionality in the ST.

New Hardware:

Series Identifier	Hardware Models
Aruba 8325 Switch Series	JL624A - Aruba 8325-48Y8C 48p 25G SFP/+/28 8p 100G QSFP+/28 Front-to-Back 6 Fans and 2 PSU Bundle (JL635A chassis) JL625A - Aruba 8325-48Y8C 48p 25G SFP/+/28 8p 100G QSFP+/28 Back-to-Front 6 Fans and 2 PSU Bundle (JL635A chassis) JL626A - Aruba 8325-32C 32-port 100G QSFP+/QSFP28 Front-to-Back 6 Fans and 2 PSU Bundle (JL636A chassis) JL627A - Aruba 8325-32C 32-port 100G QSFP+/QSFP28 Back-to-Front 6 Fans and 2 PSU Bundle (JL636A chassis)

The 8325 series uses a Xeon processor with the Broadwell microarchitecture. It runs the same software as the existing platforms and has the same interfaces as those already evaluated. As such, there are no security differences in this platform and the CAVP certificates remain valid.

Bug Fixes:

These defects were primarily functional in nature and none has any bearing on the security requirements in the evaluated ST.
The bug fixes are listed 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 hardware series and version number
Guidance Documentation: • Aruba, a Hewlett Packard Enterprise Company Common Criteria Admin Guide, Version 1.1, October 24, 2019	• Release Notes to address version • Aruba, a Hewlett Packard Enterprise Company Common Criteria Admin Guide, Version 1.3, March 26, 2019

Regression Testing:

Aruba has performed regression testing on 10.02 on both the new and old 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 testing during 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 2/19/2019. No public 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. While the updated TOE now supports TLS security for Syslog configuration, this feature was not part of the original evaluation and has not been assessed in the maintenance update. 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.