ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
Aruba, a Hewlett Packard Enterprise Company 6200, 6300, 6400, 8320, 8325, 8360, and 8400 Switch Series

Aruba, a Hewlett Packard Enterprise Company 6200, 6300, 6400, 8320, 8325, 8360, and 8400 Switch Series

Maintenance Report Number: CCEVS-VR-VID11195-2022

Date of Activity: 22 March 2022

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 "Aruba, a Hewlett Packard Enterprise Company 6200, 6300, 6400, 8320, 8325, 8360, and 8400 Switch Series" to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 25 February 2022. 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 consisted of the Security Target (ST), the Operational User Guide, and the Impact Analysis Report (IAR). The ST and User Guide were updated, and the IAR was new.

Documentation updated:

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: Aruba, a Hewlett Packard Enterprise Company 6200, 6300, 6400, 8320, 8325, 8360, and 8400 Switch Series Security Target, Version 0.6,	The ST was updated to reflect TOE version 10.09.

February 4, 2022	
Guidance: Common Criteria Admin Guide, Network Device collaboration Protection Profile, Target of Evaluation: Aruba 6200, 6300, 6400, 8320, 8325, 8360, and 8400 Switch Series, Version 2.0, February 4, 2022	The CC Configuration Guide was updated to reflect TOE version 10.09.

Changes to the TOE:

Each of the changes to "Aruba, a Hewlett Packard Enterprise Company 6200, 6300, 6400, 8320, 8325, 8360, and 8400 Switch Series" fell into the following categorization:

Major Changes

None.

Minor Changes

The TOE was revised from the evaluated ArubaOS-CX version 10.06 to version 10.09.

1 Hardware changes – there were no hardware changes,
2 New non-security features, and
3 Bug Fixes.

Twenty-eight new features were introduced for functions that were outside the scope of the evaluation.

New Features	Assessment
CDP	The CDP protocol is outside the scope of the NDcPP22e evaluation.
DHCP Server	The TOE as a DHCP server is not part of the NDcPP22e evaluation.
SNMP	SNMP functions are outside the scope of the NDcPP22e evaluation.
New Commands	These commands only show non-NDcPP22e data. All required commands were evaluated and documented.
Access Related Updates	All of these functions are outside the scope of the NDcPP22e evaluation.
Analytics	Analytics are outside the scope of the NDcPP22e evaluation.

QoS - Guaranteed Minimum Bandwidth	Quality of service metrics are outside the scope of the NDcPP22e evaluation.
Mirroring	Mirroring is outside the scope of the NDcPP22e evaluation.
NetEdit updates	NetEdit is an admin tool not included in the evaluation.
Radius	Radius servers were not included in the evaluation.
Telemetry	Analysis of telemetry data was not included in the evaluation.
VSF	Stacking was not included in the evaluation.
DNS	The TOE was not evaluated for DHCP functions.
Telnet	This is an added management function and was not considered in the NDcPP22e evaluation.
VLAN	VLAN client access is outside the scope of the NDcPP22e evaluation.
Device Fingerprinting	This is an added function and was not considered in the NDcPP22e evaluation.
Light Layer 3 Switch	This is an added function and was not considered in the NDcPP22e evaluation.
OSPF	The functions of the routing OSPF protocol was not considered in the NDcPP22e evaluation.
MAC Tables	The NDcPP22e SFRs do not address MACs.
Roles	These are added management functions not required in the evaluation.
Multi Domain Authentication	This is an added function and was not considered in the NDcPP22e evaluation.
Private VLANs	This is added functionality and not in the scope of an NDcPP22e evaluation.
Transceivers	This is an added function and was not considered in the NDcPP22e evaluation.
802.1X authentication	The 802.1X protocol was not in the NDcPP22e evaluation
ACLs	The ACL timer has no impact on the NDcPP22e requirements.

IP services	None of these IP Services are related to the NDcPP22e requirements.
Multicast	Multicast does not impact any requirements in the NDcPP22e evaluation.
Routing	The NDcPP22e requirements do not address routing details so this is not applicable to the evaluation.
Miscellaneous 1. Ensure configuration integrity. 2. Limit concurrent users for web access. 3. Added a CLI command (logging threshold) to enable/disable or change the logging threshold limit. 4. Added a CLI command (show authentication locked-out users) to show locked out users. 5. Provided a mechanism to limit admin access to audit log files. 6. A switch now triggers an event log when the security logging exceeds a set threshold. 7. Added the ability to access various logs through the CLI. o Idle timeout o Limit the number of remote access sessions o Audit services: Start audit services, record for authentication events for users, enable/disable of services	1. This is an added feature that allows an admin to show a hash of the config if wanted. This was not needed to meet the NDcPP22e requirements. 2. Not evaluated as part of the NDcPP22e evaluation. 3. Not necessary to meet the NDcPP22e evaluation. 4. Not necessary to meet the NDcPP22e evaluation. 5. A new 'security-group' was added that is not used by default. Not evaluated as part of the NDcPP22e evaluation. 6. This is added feature not necessary to meet the NDcPP22e evaluation 7. This is added feature not necessary to meet the NDcPP22e evaluation a. Idle timeout – this log was always sent to syslog. b. This feature relates to the REST API which was not part of the evaluation. c. This feature made a cleaner distinction of the auditor role. This role was not covered by the NDcPP22e certification.

Twelve bug fixes were released for existing features that were outside the scope of the evaluation, or which did not directly impact any TOE security-related actions or operations.

Bug fix Category	**Assessment**
Port Access Crash bugs • Restart interface bugs • Radius related issues	All port related bugs dealt with Radius servers which are not in the scope of the evaluation.
NTP • NTP does not take into account its source IP when the loopback interface is used • NTP not working properly with DHCP	The TOE was not evaluated as an NTP server.
Logging • Filename too long when moving • Incorrect permission on local logs • warning similar to Excessive write to coredump partition in module 1/2 observed. 7.07GB written over past 1 hour is logged in the event log	These are bugs with the local log. None were noted during the NDcPP22e evaluation, and none had any effect on evaluation testing.

SNMP	There are several SNMP fixes, but that protocol was not in the NDcPP22e evaluation.
Routing protocols	There are several fixes related to the routing protocols. Those are functional in nature and not considered in the NDcPP22e evaluation.
Radius/TACACS fixes	Authentication servers were not included in the NDcPP22e evaluation.
Interfaces • Denial of service on a restart	This results in a lack of access and does not pose an issue with the NDcPP22e evaluation. A reboot reset the interface before the fix was in place.
802.1X authentication	There are several 802.1X authentication fixes but that protocol was not in the NDcPP22e evaluation.
Management related fixes • REST API updates • Diagnostic updates • Config file format updates (use Linux format) • Interfaces command displays extra information but works properly	These are management functions not included in the NDcPP22e evaluation.
ACL • SNMP ACLs not functioning properly.	SNMP was not included in the evaluation.
Counters • The switch counts CRC errors and runt packets rather than reporting collisions properly • The switch reports collision errors or collision error counters increment incorrectly	The counters were not used in meeting the NDcPP22e requirements. As such, these changes have no impact on the evaluation results.
Bluetooth • The Bluetooth device name does not change when the switch hostname is changed, maintaining existing Bluetooth connections.	Bluetooth was not included in the evaluation

Regression Testing:

Aruba performed regression testing on TOE version 10.09 on both the new and old platforms. All platforms in the ST were subject to testing. All tests completed satisfactorily.

NIST CAVP Certificates:

The existing CAVP certs were examined and found to still be valid. The hardware was not changed/added, and no software changes impacted the tested cryptographic library.

Vulnerability Analysis:

A public search was performed on 03/19/2022.

The search of the following national sites was conducted;

- The 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),
- Exploit / Vulnerability Search Engine (http://www.exploitsearch.net),
- SecurITeam Exploit Search (http://www.securiteam.com),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search), and
- Offensive Security Exploit Database (https://www.exploit-db.com/).

The following search terms were used:

- "Aruba 6200",
- "Aruba 6300",
- "Aruba 6400",
- "Aruba 8320 ",
- "Aruba 8325 ",
- "Aruba 8360",
- "Aruba 8400 ",
- "NXP 1046A",
- "Intel Atom C2538",
- "Intel Xeon D-1518 ",
- "Intel Xeon D-1527 ",
- "Yocto", and
- "OpenSSL", "", "".

Vendor:

- Aruba, a Hewlett Packard Enterprise Company

Summary of the analysis

The vulnerability search returned 73 results. The issues found were either for those where fixes have been applied, were duplicates found on the various sites searched, or were related to other products, and not applicable to the TOE.

Conclusion:

The overall impact is minor. This is based on the above rationale that new, non-security relevant, features, or bug fixes, to update the TOE to version 10/09, had no impact on the certified TOE.

In addition, a search for vulnerabilities identified none directly effecting the TOE.

Also, the developer confirmed the changed TOE conforms to NIAP Policy 5, and the existing CAVP certs were found to still be valid.

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