# ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

# Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series

---

**Maintenance Update for:** 2930F, 2930M, and 5400R Series Switches running ArubaOS 16.04

**Maintenance Report Number**: CCEVS-VR-VID10872-2019a

**Date of Activity**: 28 August 2019

**References**:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- Collaborative Protection Profile for Network Devices, Version 2.0, + Errata 20180314, 14 March 2018 (NDcPP20E)
- Impact Analysis Report for Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series, Revision 1.1, 08/27/2019
- Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08 (NDcPP20E) Security Target, Version 0.8, 08/27/19
- Common Criteria Evaluation and Validation Scheme Validation Report, Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04, Report Number CCEVS-VR-10872-2018, dated June 1, 2018, Version 0.4.

**Documentation reported as being updated**:

- Security Target – Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04 (NDcPP20E) Security Target, Version 0.6, 05/31/18 which has been updated to: Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.08 (NDcPP20E) Security Target, Version 0.8, 08/27/19
- Common Criteria Configuration Guidance Network Device Collaboration Protection Profile, Target of Evaluation: Aruba 2930F, 2930M, 3810M and 5400R Switch Series, Version 1.6, August 20, 2019

- New versions of Release Notes address the changes:
    - KB.16.05.0011 Release Notes, September 2018, Edition: 1
    - KB.16.06.0008 Release Notes, September 2018, Edition: 1
    - KB.16.07.0002 Release Notes, September 2018, Edition: 1
    - KB.16.08.0001 Release Notes, November 2018, Edition: 1
    - WC.16.05.0011 Release Notes, September 2018, Edition: 1
    - WC.16.06.0008 Release Notes, September 2018, Edition: 1
    - WC.16.07.0002 Release Notes, September 2018, Edition: 1
    - WC.16.08.0001 Release Notes, January 2019, Edition: 1

**Assurance Continuity Maintenance Report:**

On behalf of Aruba, a Hewlett Packard Enterprise Company, Gossamer Security Solutions prepared and submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 29 May 2019. An 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.

The purpose of this ACMR is to summarize and present the findings of CCEVS' analysis of the IAR and associated evidence submitted in support of the changes to the original evaluation, and to make a determination regarding the appropriateness of Assurance Maintenance Continuity for the evaluation.

**Introduction**:

VID10872, Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04 was evaluated by Gossamer Security Solutions. The product met the security requirements specified by the NIAP-approved protection profile: Collaborative Protection Profile for Network Devices + Errata 2018314, 14 March 2018.

Aruba has requested an assurance maintenance activity for the product to update the original evaluation.

**Summary Description:**

The vendor made software changes that addressed bug fixes and added new features to the software, revising it from the evaluated ArubaOS-CX version 16.04 to version 16.08. The vendor has added additional hardware configurations to the existing series of switches. The documentation

has been updated to reflect the software version numbering and hardware models as well as the publication of new Release Notes to supplement the updated Security Target and Common Criteria Configuration Guide.

**Changes to TOE:**

The changes are divided into two categories: hardware and software. The TOE has been revised from the evaluated ArubaOS-CX version 16.04 to version 16.08. The subsections below provide justification that the changes have no security relevance on the certified TOE.

**Hardware Additions to TOE**:

The vendor has added additional hardware to the existing switch series. These additional platforms use the same software as others in the same series. They were addressed in regression testing and the CAVP certificates remain valid for these models.

| Series | Hardware Models | Processor |
|---|---|---|
| Aruba 2930F Switch Series | 2930F 24G PoE+ 4SFP+ Switch (JL255A)<br>2930F 48G PoE+ 4SFP+ Switch (JL256A)<br>2930F 24G 4SFP Switch (JL259A)<br>2930F 48G 4SFP Switch (JL260A)<br>2930F 24G PoE+ 4SFP Switch (JL261A)<br>2930F 48G PoE+ 4SFP Switch (JL262A)<br>2930F 48G PoE+ 4SFP 740W Switch (JL557A)<br>2930F 48G PoE+ 4SFP+ 740W Switch (JL558A)<br>2930F 48G PoE+ 4SFP+ 740W Switch (JL559A) | Dual Core ARM Coretex |
| Aruba 2930M Switch Series | 2930M 40G 8 HPE Smart Rate PoE Class 6 1-slot Switch (R0M67A)<br>2930M 24 HPE Smart Rate PoE Class 6 1-slot Switch (R0M68A) | Dual Core ARM Coretex |

**Software Changes to TOE**:

The changes are divided into several categories: New Non-Security Related Features, Security Related Additions, and Bug Fixes. The subsections below help to justify that the changes have no security impact on the certified TOE.

**New Non-Security Related Features**

Features and enhancements have been added to the updated software. See the following table for an analysis of each feature.

| 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 evaluation. |
| Aruba Central support added - The switch Web GUI now includes a page to help customers to onboard their switches to Aruba Central | Onboarding with Aruba is outside the scope of the NDcPP evaluation. |
| • BGP connections over GRE tunnels<br>• IPv6 multicast routing<br>• Multi-protocol BGP (IPv6 routing)<br>• Multicast routing - Loopback for RP and BSR is now supported for both IPv4 and IPv6.<br>• Policy Based Routing (PBR) - a flexible feature for creating various routing decisions based on additional information in the packets. | Routing features are outside the scope of the NDcPP evaluation. |
| Control plane ACLs - Control plane ACLs control access to the control plane | ACLs are outside the scope of the NDcPP evaluation. |
| Egress queue shaping - limits the amount of traffic transmitted per output queue | Implementation of traffic limitations is outside the scope of the NDcPP evaluation. |
| IPSLA – network monitoring | Network monitoring is outside the scope of the NDcPP evaluation. |
| • Mirror to CPU - adds the capability to mirror dataplane packets to the CPU for monitoring directly on the switch using Tshark.<br>• Remote mirroring - uses GRE encapsulated mirrored frames to a destination network device | Mirroring is outside the scope of the NDcPP evaluation. |
| • NAE encrypted credentials<br>• NAE periodic callback actions - Using the Network Analytics Engine (NAE) python API, users can set callbacks to be called in regular intervals<br>• NAE time series for external APIs- Using Network Analytics Engine (NAE) period callback actions, an NAE agent can be created using an | The Network Analytics Engine was not included in the evaluated configuration. |

| | |
|---|---|
| external API from another device or services. | |
| Multicast<br>• Storm control added<br>• Services such as self ping, telnet, SSH, and WebUI support are enabled over the VRRP virtual IP address<br>• Display of more multicast statics | Multicast is outside the scope of the NDcPP evaluation. |
| Clearpass related enhancements<br>• Netdestination and Netservice is now supported with Downloadable User Roles for all class policies configured on Aruba ClearPass<br>• Deploying ClearPass becomes easier as the switch automatically downloads the root CA certificate from ClearPass | Interaction with Clearpass is outside the scope of the NDcPP evaluation |
| 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. The NTP internal NTP server is not used in the evaluation. |
| Object groups for ACLs - This feature enables the creation of named groups representing sets of IPv4 or IPv6 addresses and L4 port ranges. | ACLs are outside the scope of the NDcPP evaluation. |
| Port Security - Enabled auto recovery of port security on an error-disabled port. With this feature, the port-security error-disabled port can be re-enabled after a specified disable time period | Port security is outside the scope of the NDcPP evaluation. |
| Rest Interface –<br>• The ability for REST clients to use RADIUS/TACACS+ for authorization instead of using per-switch passwords has been added<br>• Additional interfaces have been added | Rest Interface is outside the scope of the NDcPP evaluation in the evaluated configuration. The Admin Guide has been updated to specifically exclude it in the "Disabling Services Not Under Evaluation" section. |
| Rx Flow Control - Frames received on a port will pause sending egress packets. | Flow control is outside the scope of the NDcPP evaluation |

| | |
|---|---|
| When the pause timer expires, the transmission of packets will proceed | |

**Security related additions:**

| | |
|---|---|
| • RADIUS accounting, addressing, third party/legacy support, server groups<br>• PKI for syslog,<br>• TACACS+ servers support in a IPv6 deployment added<br>• ServiceOS console password have been added to enhance security on the switch<br>• Customers will now be able to precisely control the order in which different authentication methods are attempted<br>• AOS-Switch now allows device level configurations to be added to User Roles<br>• Max number of roles added | • RADIUS, TACACS+ and syslog PKI– these were not in the scope of the NDcPP evaluation.<br>• 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.<br>• Only password authentication was in the evaluation scope.<br>• Device level configurations were not in the NDcPP evaluation scope<br>• Roles addition is a performance issue. No new roles were added. This change simply limits the number of users that can be assigned to existing roles to 512. |
| SmartRate - There is 100 Mbps support on Smart Rate ports | Performance issues are outside the scope of the NDcPP evaluation. |
| 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. |
| Traffic policing - This allows the user to specify two rates: a commit rate and a peak rate, and associated actions which will be applied to traffic which exceeds each rate. | Performance issues are outside the scope of the NDcPP evaluation. |
| Uplink Failure Detection - allows downlink ports to be disabled if the uplink connection fails to aid in faster detection of failure | Performance issues are outside the scope of the NDcPP evaluation. |
| User based tunneling - allow customers to deploy the feature without the need for VLAN synchronization across the switch and the controller, simplifying the deployment | User based tunneling is outside the scope of the NDcPP evaluation. |

| | |
|---|---|
| VOIP - customers can bypass authentication for certain wired devices such as VoIP phones while still allowing the clients behind the phones to authenticate | VOIP is outside the scope of the NDcPP evaluation |
| VSX Features – Expands spanning tree interoperability | VSX is outside the scope of the NDcPP evaluation. |
| Switches can now use their OOBM ports to check-in with AirWave. Note that the feature supports only the DHCP based ZTP mechanism with AirWave. | ZTP and Airwave outside the scope of the NDcPP evaluation. |

**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. There are several bugs identified as being part of the security group and are shown below:

| **Bug Fix** | **Assessment** |
|---|---|
| Symptom/Scenario: After switch upgrade, when the self-signed certificate is generated, the connection to the switch cannot be established via web server using HTTPS. Workaround: Downgrade to the lower version, generate the self-signed certificate from that build and use this generated certificate in the upgraded build. | This is a denial of service issue. When certificates are installed, they work properly. |
| Symptom: Unable to establish SSH connections to the switch.<br>Scenario: Over time, the switch may become unable to accept SSH connections. When attempting to access the switch console interface, it may crash with an error message similar to Unable to get semaphore for Server | This is a denial of service issue. The switch can be rebooted. |

**Affected Developer Evidence**:

Modifications were made to the ST to change the software version and to add the new hardware models. The Release Notes were updated to address version number and features. The Common

Criteria Guidance was updated to address the new hardware models, version numbers and other non-security relevant features.

**Regression Testing**:

Aruba has performed regression testing on 16.08 on all platforms. The additional platforms were addressed in regression testing and the CAVP certificates remain valid for these models.

**Vulnerability Analysis**:

The updates to software included security relevant fixes for documented CVEs. The CVE databases were searched on 5/28/2019 and again on 8/6/2019 to ensure known security vulnerabilities have been corrected.

The evaluator searched the following:

- 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),
- Offensive Security Exploit Database (https://www.exploit-db.com/) on 4/24/2019,

using the following search terms: : "TCP", "Hpe aruba", "3810m ", "2930f", "2930m", “5400r”, "SSH", "TLS", "switch", "Mocana”.

The search resulted in 570 findings, most of those were due to the generic nature of the search terms “switch” and “TLS”. None of the 570 findings were found to be applicable to the TOE. 549 findings were related to other products and not applicable to the TOE, the remaining 21 findings were duplicates among the searched databases.

**Conclusion**:

CCEVS reviewed the vendor provided description of the analysis of the devices and found there to be only **minor** impact upon security related functionality. In addition, the TOE vendor reported having conducted a vulnerability search update 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. Therefore, CCEVS agrees that the original assurance is maintained for the product.