National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
for the
Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10

Report Number: **CCEVS-VR-VID11403-2023**

Dated: **November 20, 2023**

Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson

Randy Heimann

Lisa Mitchell

Clare Parran

Lori Sarem

Chris Thorpe

The MITRE Corporation

Common Criteria Testing Laboratory

Sean Bennett

Greg McLearn

Kevin Steiner

Wasif Sikder

Lightship Security USA, Inc.

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 provided by Aruba, A Hewlett Packard Enterprise Company. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in November 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 (CFG_NDcPP-VPNGW_V1.2). This PP-Configuration includes the following components:

> Base PP: collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
>
> PP-Module: PP-Module for Virtual Private Network (VPN) Gateways, Version 1.2 (MOD_VPNGW_V1.2)

The TOE is Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Security Target, v1.6, November 2023*, and analysis performed by the Validation Team.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10
Sponsor and Developer	Aruba, A Hewlett Packard Enterprise Company 6280 America Center Dr. San Jose, CA 95002
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

Item	Identifier
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.
Protection Profile	PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways, Version 1.2, 31 March 2022 (CFG_NDcPP-VPNGW_V1.2). This PP-Configuration includes the following components: Base PP: collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E) PP-Module: PP-Module for Virtual Private Network (VPN) Gateways, Version 1.2 (MOD_VPNGW_V1.2)
ST	*Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Security Target*, v1.6, November 2023
Evaluation Technical Report	*Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Evaluation Technical Report*, Version 1.3, November 14, 2023
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Sean Bennett, Greg McLearn, Kevin Steiner, Wasif Sikder
CCEVS Validators	Jenn Dotson, Randy Heimann, Lisa Mitchell, Clare Parran, Lori Sarem, Chris Thorpe

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is a distributed network security solution offered by Aruba, a Hewlett Packard Enterprise company and is comprised of Aruba Remote Access Points (RAP) and an Aruba Mobility Controller (each with an embedded ArubaOS). The TOE devices are running ArubaOS 8.10. The Mobility Controller provides VPN gateway functionality for gateway-to-gateway VPN connections. The RAP and Mobility Controller communicate via IPsec.

3.1. TOE Evaluated Configuration

The TOE is deployed in a distributed configuration with the Aruba Remote Access Points providing connectivity for wireless clients in a branch deployment, and the Aruba Mobility Controller serving as a gateway between wired and wireless networks as well as command and control functionality over Aruba RAPs.

The TOE interfaces are as follows:

a) **CLI.** Local serial and remote SSH command line interface.

   Note: The SSH channel can be tunneled over IPsec.

b) **GUI.** Web-based management UI via HTTPS/TLS.

   Note: This channel can be optionally tunneled over IPsec and was tested in this evaluation.

c) **RAP IPsec.** Secure tunnel between RAP and Mobility Controller via IPsec (TOE acts as peer).

d) **RADIUS/TACACS+.** Authentication servers for user authentication via IPsec (TOE is VPN gateway).

e) **NTP.** The TOE synchronizes time with an NTP server via IPsec (TOE is VPN gateway).

f) **Syslog.** Interface for sending audit logs to remote audit server via IPsec (TOE is VPN gateway).

g) **OCSP.** The TOE receives certificate revocation status information from an external OCSP responder.

3.2. Physical Boundary

The physical boundary of the TOE includes the appliance models shown in Table 2 executing ArubaOS 8.10 software. The ArubaOS consists of a base software package with add-on software modules that can be activated by installing the appropriate licenses. The following modules are required to be licensed and activated in the CC evaluated configuration:

- **Policy Enforcement Firewall Next Generation.** Provides identity-based security for wired and wireless clients.

- **Advanced Cryptography.** Required for Commercial National Security Algorithms Suite, AES-GCM, and ECDSA functionality.

Table 2: TOE models

Type	Model	CPU	Software
Mobility Controller	7210	Broadcom XLP416 (MIPS64)	ArubaOS 8.10
Mobility Controller	7220	Broadcom XLP432 (MIPS64)	
Mobility Controller	9004	Intel Atom C3508 (Denverton)	
Remote Access Point	303H	Qualcomm IPQ4019 (ARM Cortex-A7)	
Remote Access Point	503H	Broadcom BCM47622L (ARM-A7)	
Remote Access Point	505H	Broadcom BCM47622L (ARM-A7)	

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

a) **Audit Server.** The TOE sends audit events to a remote syslog server.

b) **NTP Server.** The TOE synchronizes time via NTP.

c) **Authentication Server.** The TOE leverages a RADIUS or TACACS+ server for handling user authentication.

d) **OCSP Responder.** The TOE receives certificate revocation status information from an external OCSP responder.

e) **Administrator Workstation.** The device(s) used by administrators to facilitate access to the TOE CLI and GUI interfaces.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Security Audit

The TOE generates logs for security relevant events including startup and shutdown of the TOE and all administrative actions. Logs are stored locally on the Mobility Controller to be accessed by an administrator or can be configured to be sent via syslog to a remote server in the operational environment.

4.2. Cryptographic Support

The TOE implements key generation, establishment, and other cryptographic services to protect data in transit and at rest within the TOE. In support of cryptographic functions, the TOE implements two cryptographic modules that perform all IPsec/IKE session operations, and functions that support all SSH, HTTPS, and TLS operations. The relevant Cryptographic Algorithm Validation Program (CAVP) certificates have been obtained for the necessary components.

4.3. Communication

The TOE is a distributed configuration consisting of an Aruba Mobility Controller and Aruba RAPs. The Security Administrator must enable communications between the RAPs and Controller TOE components before any communication can take place. The RAPs must be configured with an appropriate RSA or ECDSA certificate and the IP address of the Aruba Mobility Controller.

4.4. Identification and Authentication

The TOE implements mechanisms to identify and authenticate administrators to ensure only authorized access to TOE functionality or TSF data is granted. These mechanisms can also be implemented using RADIUS or TACACS+ servers within the operational environment.

4.5. Security Management

The TOE provides the administrator role with the capability to configure and manage all TOE security functions including cryptographic operations, user accounts, passwords, advisory banner, session inactivity, and TOE updates. The management functions are restricted to the administrator role which must be assigned to an administrative user or access to these functions will be denied.

4.6. Packet Filtering

The TOE acts as a VPN gateway – a device at the edge of a private network that terminates an IPsec tunnel, which provides device authentication, confidentiality, and integrity of information traversing a public or untrusted network. The TOE provides packet filtering for gateway-to-gateway VPN connections. Administrators can configure security policies that determine whether to block, allow, or log a session based on traffic attributes such as source and destination port, IP address or service.

4.7. Protection of the TSF

The TOE implements a variety of protection mechanisms including authentication, self-tests, and reliable timestamping that leverages an internal hardware clock, or synchronization with an NTP server. Passwords are stored on flash using SHA1 hashes and the TOE does not provide an interface that allows for passwords or keys to be read. Confidentiality and integrity are provided for all communications between TOE components via IPsec.

4.8. TOE Access

The TOE provides session monitoring and management functions for local and remote administrative sessions. A warning banner is displayed at the management interfaces (Web GUI and CLI) to advise users on appropriate use and penalties for misuse of the system.

4.9. Trusted Path/Channels

The TOE provides secure channels between itself and local/remote administrators, including logging channels to ensure data in transit is protected. IPsec is implemented to provide encrypted channels between Mobility Controllers and third-party trusted IT entities in the operating environment. The TOE also uses IPsec to encrypt communications between TOE components and for all VPN connections. Remote Web UI access is protected with TLS/HTTPS, and CLI access is protected via SSHv2.

5. Assumptions and Clarification of Scope

5.1. Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *collaborative Protection Profile for Network Devices*, v2.2e, 23 March 2020 (CPP_ND_V2.2E)
- *PP-Module for Virtual Private Network (VPN) Gateways*, Version 1.2, 31 March 2022 (MOD_VPNGW_V1.2)

That information has not been reproduced here and the CPP_ND_V2.2E and MOD_VPNGW_V1.2 should be consulted if there is interest in that material.

5.2. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V2.2E and MOD_VPNGW_V1.2 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made in accordance with the evaluation activities specified in CPP_ND_V2.2-SD and MOD_VPNGW_V1.2-SD and performed by the Evaluation team
- This evaluation covers only the specific software version identified in this document and referenced in the *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Security Target*, Version 1.6, November 2023, and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific software version and platform versions was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_ND_V2.2E, MOD_VPNGW_V1.2 and

applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Common Criteria Configuration Guidance ArubaOS 8.10 Supplemental Guidance (Target of Evaluation: Aruba Remote Access Points with Mobility Controllers running ArubaOS 8.10-FIPS), Version 2.3, November 2023*
- *ArubaOS 8.10.0.0 User Guide, Revision 14, 2023*
- *ArubaOS 8.x Command-Line Interface Reference Guide, 2023*
- *ArubaOS 8.10.0.0 Syslog Reference Guide*
- *Aruba 303H Series Hospitality Access Points Installation Guide, March 2017*
- *Aruba 503H Series Hospitality Access Points Installation Guide, July 2020*
- *Aruba AP-505H Access Points Installation Guide, May 2023*
- *Aruba 7200 Series Controller Installation Guide 0511169-06, July 2015*
- *Aruba 9004 Gateway Installation Guide, Revision 03, June 2021*

To use the product in the evaluated configuration, the product must be installed and configured as specified in *Common Criteria Configuration Guidance ArubaOS 8.10 Supplemental Guidance (Target of Evaluation: Aruba Remote Access Points with Mobility Controllers running ArubaOS 8.10-FIPS)*. This document provides references to other documentation for specific steps to place the TOE into its the evaluated configuration and these documents are provided on the NIAP website.

7. IT Product Testing

This section describes the testing efforts of the Evaluation team. It is derived from information contained in *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Assurance Activity Report (AAR)*, Version 1.3, November 14, 2023, and the proprietary *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Detailed Test Report (DTR)*, Version 1.4, November 14, 2023, and *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Detailed Test Report Evidence*, Version 1.4, November 14, 2023.

7.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities for this product.

7.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from December 2022 until November 2023. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

7.3. Evaluated Configuration

The TOE testing environment components are identified in Figure 1 below.

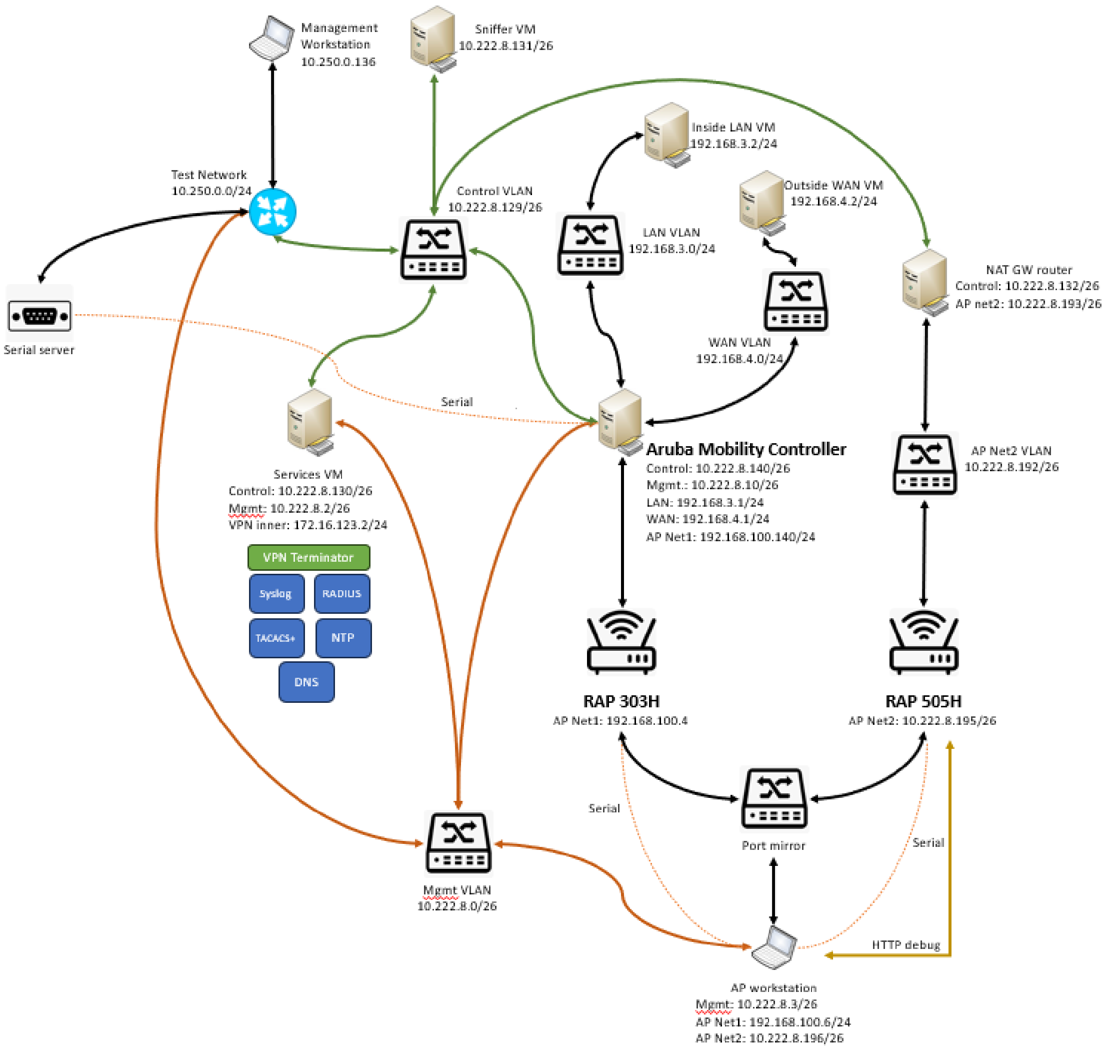

Figure 1: Testing Environment Overview

8. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary DTR & ETR. The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5 and the specific evaluation activities specified in CPP_ND_V2.2-SD and MOD_VPNGW_V1.2-SD.

The Evaluation determined the TOE satisfies the conformance claims made in the *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Security Target, v1.6, November 2023* of Part 2 extended and Part 3 conformant. The Validation Team reviewed all the work of the Evaluation team and agreed with their practices and findings.

8.1. Evaluation of Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a ST introduction, TOE overview, TOE description, description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.2. Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed Protection Profile for design evidence. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the Evaluation Activities related to the examination of the information contained in the TSS.

The Validation reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.3. Evaluation of Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.5. Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Test Evaluation Activities and recorded the results in a Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Vulnerability Assessment*, Version 0.2, November 2023, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on October 31, 2023, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures:
    - http://cve.mitre.org/cve/
    - https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security: https://www.tenable.com/cve
- Tipping Point Zero Day Initiative: http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/

- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

The Evaluation team performed a search using the following keywords:

- Aruba Mobility Controller
- Aruba Remote Access Point
- ArubaOS 8.10
- Aruba Crypto Module
- Aruba OpenSSL Module
- Aruba Bootloader Module
- Aruba 303H
- Aruba 503H
- Aruba 505H
- Aruba 7210
- Aruba 7220
- Aruba 9004
- Broadcom XLP416
- Broadcom XLP432
- Intel Atom C3508
- Qualcomm IPQ4019
- Broadcom BCM47622L
- FreeRADIUS
- Ntp.org
- Mocana
- OpenSSH
- OpenSSL

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.7. Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM and performed the Evaluation Activities in CPP_ND_V2.2-SD and MOD_VPNGW_V1.2-SD, and correctly verified that the product meets the claims in the ST.

9. Validator Comments

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Customers should be aware that the TOE requires the purchase of two additional license-restricted modules, which must be activated in the evaluated configuration as described in the ST. They are the Policy Enforcement Firewall Next Generation and the Advanced Cryptography modules.

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in *Common Criteria Configuration Guidance ArubaOS 8.10 Supplemental Guidance (Target of Evaluation: Aruba Remote Access Points with Mobility Controllers running ArubaOS 8.10-FIPS)*. As noted in Section 6, consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated. No versions of the TOE and software, either earlier or later were evaluated.

Any additional customer documentation, not listed in Section 6, provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore, should not be relied upon to configure or operate the TOE as evaluated.

10. Annexes

Not applicable.

11. Security Target

Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Security Target, v1.6, November 2023

12. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance:** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature:** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. Acronym List

AAR	Assurance Activity Report
CAVP	Cryptographic Algorithm Validation Program
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
DTR	Detailed Test Report
LS	Lightship Security USA CCTL
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

14. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001,* Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002,* Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003,* Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004,* Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Network Devices*, v2.2E, 23-March-2020
6. *PP-Module for VPN Gateways,* Version: 1.2, 2022-03-31
7. *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Security Target,* Version 1.6, November 2023
8. *Common Criteria Configuration Guidance ArubaOS 8.10 Supplemental Guidance (Target of Evaluation: Aruba Remote Access Points with Mobility Controllers running ArubaOS 8.10-FIPS), Version 2.3, November 2023*
9. *ArubaOS 8.10.0.0 User Guide, Revision 14, 2023*
10. *ArubaOS 8.x Command-Line Interface Reference Guide, 2023*
11. *ArubaOS 8.10.0.0 Syslog Reference Guide*
12. *Aruba 303H Series Hospitality Access Points Installation Guide, March 2017*
13. *Aruba 503H Series Hospitality Access Points Installation Guide, July 2020*
14. *Aruba AP-505H Access Points Installation Guide, May 2023*
15. *Aruba 7200 Series Controller Installation Guide 0511169-06, July 2015*
16. *Aruba 9004 Gateway Installation Guide, Revision 03, June 2021*
17. *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Evaluation Technical Report,* Version 1.3, November 14, 2023
18. *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Assurance Activity Report*, Version 1.3, November 14, 2023, and the proprietary *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Detailed Test Report* , Version 1.4, November 14, 2023 and *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Detailed Test Report Evidence*, Version 1.4, November 14, 2023
19. *Aruba Remote Access Points and Aruba Mobility Controllers with ArubaOS 8.10 Vulnerability Assessment,* Version 0.2, November 2023