National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec

Report Number: CCEVS-VR-VID11422-2024
Dated: April 22, 2024
Version: 0.4

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

James Donndelinger
Marybeth Panock
Meredith Martinez
Fernando Guzman
The Aerospace Corporation

Anne Gugel
Robert Wojcik
Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Dip Pudasaini
Cornelius Haley
Will Micknick
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec solution provided by Aruba, a Hewlett Packard Enterprise Company. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in April 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. 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 Devices and MACsec Ethernet Encryption, Version 1.0, 29 March 2023 which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10).

The Target of Evaluation (TOE) is the Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec running Aruba OS-CX version 10.11.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory 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 Validation Report 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 and the conclusions of the testing laboratory in the evaluation technical report 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec Security Target, version 1.0, April 10, 2024 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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (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, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec (Specific models identified in Section 8)
Protection Profile	PP-Configuration for Network Devices and MACsec Ethernet Encryption, Version 1.0, 29 March 2023 which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10)
ST	Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec Security Target, version 1.0, April 10, 2024
Evaluation Technical Report	Evaluation Technical Report for Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec, version 0.3, April 15, 2024
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Aruba, a Hewlett Packard Enterprise Company
Developer	Aruba, a Hewlett Packard Enterprise Company
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	James Donndelinger, Marybeth Panock, Meredith Martinez, and Fernando Guzman – The Aerospace Corporation

Item	Identifier
	Anne Gugel and Robert Wojcik – Johns Hopkins University Applied Physics Laboratory

3 Architectural Information

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

The Target of Evaluation (TOE) is Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec running Aruba OS-CX version 10.11.

The TOE offers comprehensive Layer 2 and Layer 3 features. The Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series provides security and scalability for enterprise edge deployments.

3.1 TOE Description

The TOE is a family of switches designed to support scalability, security and high performance for campus networks.

For the purpose of evaluation, the TOE will be treated as a network device offering CAVP tested cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to transmit audit records). The scope of the evaluation is limited to the NDcPP22e and MACSEC10 requirements. Functions outside the scope of the NDcPP22e and MACSEC10 were not evaluated.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 TOE Architecture

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, processor and software that implements switching functions, configuration information and drivers. While hardware varies between different appliance models, the software code is shared across all platforms. It is in the software code that all the security functions claimed this security target are enforced.

3.4 Physical Boundaries

Each TOE appliance runs the 10.11 version of the Aruba OS-CX software and has physical network connections to its environment to facilitate the switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external SYSLOG server in the network environment.

Figure 1 shows the TOE depicted in its intended environment.

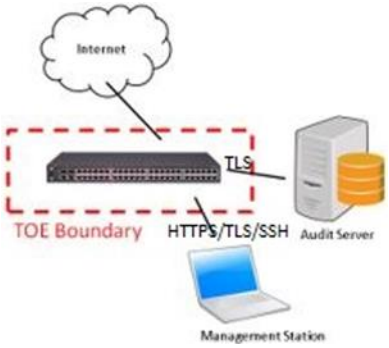

Figure 1: TOE Environment

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The TOE is able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using TLS to protect the logs while in transit on the network.

4.2 Cryptographic support

The TOE provides CAVP certified cryptography in support of its SSHv2, TLS v1.2 and MACsec protocol implementations. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature and secure hashing.

4.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching rules and reading the login banner. It provides the ability to both assign attributes (user names, passwords and roles) and to authenticate users against these attributes.

4.4 Security management

The TOE provides Command Line Interface (CLI) commands and an HTTP over TLS (HTTPS/TLS) Graphical User Interface (GUI) to access the wide range of security management functions to manage its security policies. The TOE also offers HTTPS/TLS protection for REST API interfaces that can be used for administration. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of roles that can be assigned to TOE users. The TOE supports the following roles: Administrators, Operators. The Administrator role can make changes to the TOE configuration while the Operator role is a read-only role.

4.5 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features. The TOE protects stored passwords and cryptographic keys so they are not directly accessible in plaintext. The TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment by providing a hardware clock and the ability to synchronize with the network time server. The TOE employs both dedicated communication channels as well as cryptographic means to protect communication between itself and other components in the operating environment. The TOE performs self-tests to detect failure and protect itself from malicious updates.

4.6 TOE access

The TOE can be configured to display a logon banner before and after (a post-login banner) a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

4.7 Trusted path/channels

The TOE protects communication channels between itself and remote administrators using HTTPS/TLS and SSH. The SSH protocol is used to protect administrative connections utilizing the TOE's command line interface (CLI). Additionally, web-based GUI and REST API interfaces are available for remote administration which are protected using HTTPS/TLS.

The TOE protects communication with network peers, such as a log server, using TLS connections to prevent unintended disclosure or modification of logs. The TOE supports MACsec communication with MACsec peers.

5 Assumptions & Clarification of Scope

Assumptions

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

- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)
- PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10)

That information has not been reproduced here and the NDcPP22e and MACSEC10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e and MACSEC10 as described for this TOE in the Security Target. 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.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and the MACsec Module and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific MACsec Ethernet Encryption models was not included in the scope of the evaluation and therefore should not to 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 NDcPP22e and MACSEC10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Common Criteria Administrator Guidance, Target of Evaluation: Aruba 6300M and 8360v2 Switch Series, Version 2.5, April 4, 2024

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec, Version 0.2, April 4, 2024 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e and MACSEC10 including the tests associated with optional requirements. The AAR, in section 3.4.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The evaluated configuration includes the following devices:

Series Identifier	Processor	Embedded MACsec Hardware
Aruba 6300M	NXP 1046A – ARM Cortex A72	BCM 82399 BCM 54998SM BCM 82756 BCM 82759
Aruba 8360v2	NXP 1046A – ARM Cortex A72	BCM 82399 BCM 82398

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance 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 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e and MACSEC10.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP22e and MACSEC10 related to the examination of the information contained in the TSS.

The validator 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.

9.3 Evaluation of the 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 of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator 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.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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.

9.5 Evaluation of the 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 assurance activities in the NDcPP22e and MACSEC10 and recorded the results in a Test Report, summarized in the AAR.

The validator 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.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities and fuzz testing. None of the public search for vulnerabilities or the fuzz testing uncovered any residual vulnerability.

On 4/3/2024, the evaluator searched the following sources:

- 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)
- cve.org CVE Database (https://www.cve.org/)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The search was conducted with the following search terms:

- “ArubaOS”, “AOS 10.11”, “macsec”, “TLS”, “SSH”, “Cortex A9”, “NPX 1046A”, “Xeon D-1518”, “Xeon D-1527”, “Xeon D-1637”, “Atom C2538”, “AOS-CX Cryptographic Module”, “AOS-CX RSA Engine”

The validator 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.

9.7 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 testing 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 correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

All validator comments are addressed in other sections of this Validation Report.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec Security Target, Version 1.0, April 10, 2024*.

13 Glossary

The following definitions are used throughout this document:

- **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.
- **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.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e).

[5] PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10).

[6] Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec Security Target, Version 1.0, April 10, 2024 (ST).

[7] Assurance Activity Report for Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec, Version 0.3, April 15, 2024 (AAR).

[8] Detailed Test Report for Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec, Version 0.2, April 4, 2024 (DTR).

[9] Evaluation Technical Report for Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec, Version 0.3, April 15, 2024 (ETR).