National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report
for
HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0

Report Number: CCEVS-VR-VID11689-2026
Dated: October 19, 2026
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
Sheldon Durrant
Lisa Mitchell
Clare Parran
Jaemond Reyes
Lori Sarem

The MITRE Corporations

Common Criteria Testing Laboratory

Brandan deGuzman
Douglas Kalmus
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 4
3.1 TOE Description 4
3.2 TOE Evaluated Platforms 4
3.3 TOE Architecture 4
3.4 Physical Boundaries 6
4 Security Policy 8
4.1 Security audit 8
4.2 Cryptographic support 8
4.3 Identification and authentication 8
4.4 Security management 8
4.5 Protection of the TSF 9
4.6 TOE access 9
4.7 Trusted path/channels 9
5 Assumptions & Clarification of Scope 10
5.1 Assumptions 10
5.2 Clarification of scope 10
6 Documentation 11
7 IT Product Testing 12
7.1 Developer Testing 12
7.2 Evaluation Team Independent Testing 12
8 Evaluated Configuration 13
9 Results of the Evaluation 14
9.1 Evaluation of the Security Target (ASE) 14
9.2 Evaluation of the Development (ADV) 14
9.3 Evaluation of the Guidance Documents (AGD) 14
9.4 Evaluation of the Life Cycle Support Activities (ALC) 15
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 15
9.6 Vulnerability Assessment Activity (VAN) 15
9.7 Summary of Evaluation Results 16
10 Validator Comments/Recommendations 17
11 Annexes 18
12 Security Target 19
13 Glossary 20
14 Bibliography 21

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0 solution provided by Hewlett Packard Enterprise. 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 Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in October 2026. 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:

- *Collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023 (NDcPP30e) and
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 (SSH10).

The TOE is the HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0. The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (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 *HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0 Security Target*, Version 1.0, October 15, 2026 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 Accreditation 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	HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0
Protection Profile	*collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 (NDcPP30e) and the *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10)
ST	*HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0 Security Target*, Version 1.0, October 15, 2026
Evaluation Technical Report	*Evaluation Technical Report for HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0*, version 0.3, October 15, 2026
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	Hewlett Packard Enterprise

Item	Identifier
Developer	Hewlett Packard Enterprise
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Clare Parran, Jaemond Reyes, Lori Sarem

3 Architectural Information

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

The TOE is HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0. The TOE is a network device. The HPE Networking Hardware Mobility Conductor Series provides a single management layer for all HPE Networking Mobility Controllers in a high scale enterprise environment.

3.1 TOE Description

The HPE Networking Hardware Mobility Conductor Series delivers the full capabilities of the HPE Networking Wireless Operating System to scale to today's enterprise needs. The Conductor enables high scale and reliability, managing up to 100,000 clients, 10,000 access points (APs) and 1,000 controllers/gateways. It also provides simplified deployment with dynamic license management, configuration hierarchy and a choice of x86 hardware appliances.

The HPE Networking Hardware Mobility Conductor Series is deployed as a conductor controller for any combination of MCR hardware appliances.

The Conductor increases scale by joining HPE Aruba Networking controllers to a Controller Cluster, improves reliability using enhanced high availability (HA), adopts configurations seamlessly based on hierarchy, and reduces or eliminates maintenance windows by enabling live upgrades.

3.2 TOE Evaluated Platforms

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

3.3 TOE Architecture

HPE Networking Mobility Conductor (MCs) are hardware appliances consisting of a multicore network processor, Ethernet interfaces, and required supporting circuitry and power supplies enclosed in a metal chassis.

The HPE Aruba Networking Wireless Operating System software running on the conductors consists of two main components:

- Control Plane (CP) – implements functions which can be handled at lower speeds such as Mobility Controller system management (CLI and Web GUI), user authentication (e.g. RADIUS), Internet Key Exchange (IKE), auditing/logging (syslog) and termination of protocols operating at the system level (e.g. SSH, TLS, NTP, etc.). The Control Plane runs the Linux operating system along with various user-space applications (described below).
- Data Plane (DP) - implements functions that must be handled at high speeds such as high-speed switching functions (forwarding, VLAN tagging/enforcement, bridging),

tunnel termination (IPsec), and cryptographic acceleration. The Data Plane runs a lightweight, proprietary real-time OS which is known as "SOS" (an acronym which used to mean "SiByte Operating System" for an earlier generation of Mobility Conductor that used the SiByte CPU). On the conductor hardware appliances, SOS runs on separate CPU cores.

The Control Plane and Data Plane are inseparable. Administrators install the conductor software by loading a single file, identified as "HPE Aruba Networking Wireless Operating System." Internally, the Conductor unpacks the software image into its various components. A given HPE Aruba Networking Wireless Operating System software image has a single version number and includes all software components necessary to operate the conductor appliances.

The CP runs the Linux OS, along with various custom user-space applications which provide the following CP functions:

- Monitors and manages critical system resources, including processes, memory, and flash
- Manages system configuration and licensing
- Manages an internal database used to store licenses, user authentication information, etc.
- Provides network anomaly detection, hardware monitoring, mobility management, wireless management, and radio frequency management services
- Provides a Command Line Interface (CLI)
- Provides a web-based (HTTPS/TLS) management UI for the MCs
- Provides authentication services for the system management interfaces (CLI, web GUI)
- Provides IPsec key management services
- Provides network time protocol service, point to point tunneling protocol services for users, layer 2 tunneling protocol services for users, SSH services for incoming management connections, SNMP client/agent services, and protocol independent multicast (routing) services for the controller
- Provides syslog services by sending logs to the operating environment

The Linux OS running on the CP is a version 4.14.181 kernel. Linux is a soft real-time, multi-threaded operating system that supports memory protection between processes. Only OS-8.13.0 provided interfaces are used, and the CLI is a restricted command set. Administrators do not have access to the Linux command shell or operating system.

All Conductor models run the same HPE Aruba Networking Wireless Operating System 8.13.0 software and include the same cryptographic modules. Regardless of the different hardware platforms, the security functionality remains the same. The differences in the platforms are in the processing speed, throughput, memory capacity, storage, physical interfaces, number of ports, etc., and are based on performance and scalability requirements.

All models run the same code with the only differences being the hardware specific code for the differently scaled hardware.

Although the TOE models have different specifications (in terms of performance and scalability), they all provide the same security functions described in the ST; therefore, they have been considered to be the same for the purposes of the evaluation.

3.4 Physical Boundaries

The TOE consists of the following components:

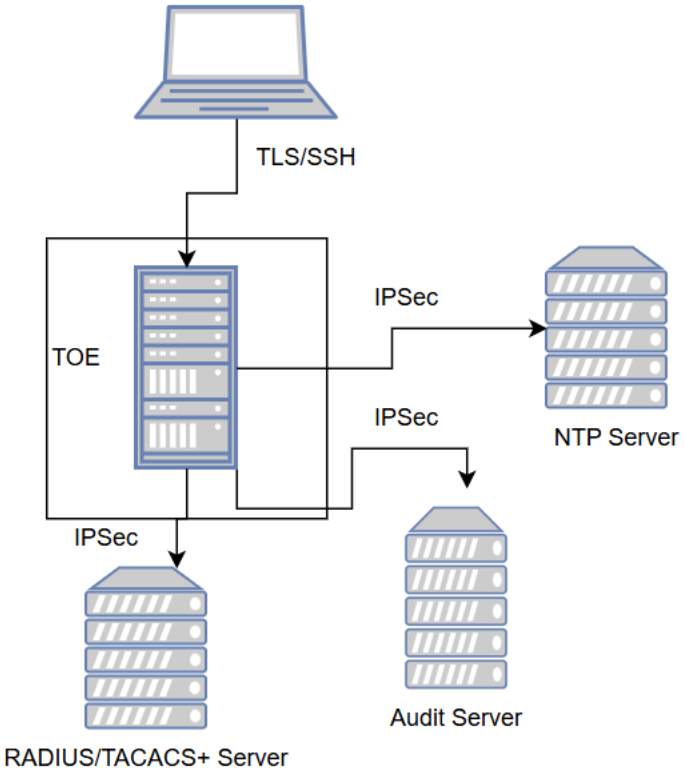
- HPE Networking Hardware Mobility Conductor Models: MCR-HW-1K, MCR-HW-5K, MCR-HW-10K
- HPE Aruba Networking Wireless Operating System version 8.13.0

These components are identified and described in Section 8 of this VR. The TOE has been evaluated as a physical device.

The HPE Aruba Networking Wireless Operating System (OS-8.13.0) consists of a base software package with add-on software modules that can be activated by installing the appropriate licenses. The following SFR-enforcing software modules are required to be licensed and installed in the CC evaluated configuration.

Required Software Module	Description
Advanced Cryptography	Required for SuiteB, AES-GCM and ECDSA functionality.

Table 1 Required Licenses



TOE Environmental Components

The TOE operates with the following components in the Operating Environment as shown in the figure above:

- Audit Server – The TOE utilizes an external syslog server to store audit records.
- Authentication Server – The TOE utilizes RADIUS and TACACs+ servers to authenticate users.
- Time Server – The TOE uses a Network Time Protocol (NTP) server to synchronize its system clock with a central time source.
- Web Browser – The remote administrator uses a web browser to access the Web GUI interface.
- SSH Client – The remote administrator uses an SSH client to access the CLI.

4 Security Policy

This section summarizes 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 designed to be able to generate logs for a wide range of security relevant events including start-up and shutdown of the TOE, all administrator actions, and all events identified in the ST. The TOE can be configured to store the logs locally so they can be accessed by an administrator or alternately to send the logs to a designated syslog server in the operational environment.

4.2 Cryptographic support

The TOE includes cryptographic modules that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher-level cryptographic protocols including IPsec, SSH, and TLS/HTTPS.

4.3 Identification and authentication

The TOE requires administrators to be identified and authenticated before they can access any TOE security functions. The TOE supports role-based authentication, so user accounts are assigned predefined roles which restrict them based on their assigned role. The TOE maintains these administrator and user attributes which can be defined locally with user names and passwords or can be defined in the context of local RADIUS or TACACS+ services. Authentication can be either locally or remotely through an external authentication server, or internally. After an administrator-specified number of failed attempts, the user account is locked out. The TOE's password mechanism provides configuration for a minimum password length. The TOE also protects, stores and allows authorized administrators to load X.509.v3 certificates for use to support authentication for IPsec connections.

4.4 Security management

The TOE provides the administrator role 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. The role must have the appropriate access privileges or access will be denied. The TOE's cryptographic functions ensure that only secure values are accepted for security attributes.

4.5 Protection of the TSF

The TOE has its own internal hardware clock that provides reliable time stamps used for auditing. The internal clock may be synchronized with a time signal obtained from an external trusted NTP server. The TOE stores passwords on flash using a SHA1 hash and does not provide any interfaces that allow passwords or keys to be read.

The TOE runs self-tests during power up and periodically during operation to ensure the correct operation of the cryptographic functions and TSF hardware. There is an option for the administrator to verify the integrity of stored TSF executable code.

The TOE includes mechanisms so that the administrator can determine the TOE version and update the TOE securely using digital signatures.

4.6 TOE access

The TOE allows administrators to configure a period of inactivity for administrator sessions. Once that time period has been reached while the session has no activity, the session is terminated. All users may also terminate their own sessions at any time. A warning banner is displayed at the management interfaces (Web GUI and CLI) to advise users on appropriate use and penalty for misuse of system.

4.7 Trusted path/channels

The TOE uses IPsec to provide an encrypted channel between itself and third-party trusted IT entities in the operating environment including external syslog server, external authentication server, and NTP server.

The TOE secures remote communication with administrators by implementing TLS/HTTPS for remote Web UI access and SSHv2 for CLI access. In each case, both the integrity and disclosure protection is ensured via the secure protocol. If the negotiation of a secure session fails or if the user cannot be authenticated for remote administration, the attempted session will not be established.

5 Assumptions & 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*, Version 3.0e, 06 December 2023 (NDcPP30e
- *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10)

That information has not been reproduced here and the NDcPP30e/SSH10 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 the NDcPP30e/SSH10 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 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 NDcPP30e/SSH10 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 identified in Section 6, additional customer documentation for the specific Network Device models 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 NDcPP30e/SSH10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following document was available with the TOE for evaluation:

- *HPE Aruba Networking Wireless Operating System 8.13.0 Supplemental Guidance (Common Criteria Configuration Guidance)*, Version 3.2, October 2026

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 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 HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0*, Version 0.3, October 115, 2026 (DTR), as summarized in the *Assurance Activity Report for HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0*, Version 0.3, October 15, 2026 (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 NDcPP30e/SSH10 including the tests associated with optional requirements. The AAR, in Sections 1.1.1 and 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 consists of the HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0 and the following required software licenses:

- Advanced Cryptography

The TOE includes the following hardware models:

Product Model	CPU
MCR-HW-1K	Intel Xeon E5-2609v4 (Broadwell)
MCR-HW-5K1	Intel Xeon E5-2620v4 (Broadwell)
MCR-HW-10K	Intel Xeon E5-2650v4 (Broadwell)

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 DTR and ETR documents. 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 HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP30e/SSH10.

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 HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0 products 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.

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 ST and Guidance document. Additionally, the Evaluation team performed the assurance activities specified in the NDcPP30e/SSH10 related to the examination of the information contained in the TSS.

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.

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. The guide was 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.

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 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.

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 NDcPP30e/SSH10 and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence was provided by the Evaluation team to show that the evaluation activities addressed the test activities in the NDcPP30e/SSH10, 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 Evaluation team. The vulnerability analysis includes a public search for vulnerabilities.

The Evaluation team searched the following public vulnerability databases:

- MITRE CVE Database, National Vulnerability Database, and CVE details (https://www.cve.org/, https://web.nvd.nist.gov/vuln/search, and https://www.cvedetails.com/vulnerability-search.php)
- Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)
- 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)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The Evaluation team performed the vulnerability searches with the following key words. The last search was performed on 10/13/2026:

“ArubaMM-HW-1K”, “Aruba Mobility Conductor”, “ArubaMM”, “ArubaOS version 8.13.0”, “ArubaOS”, “MCR-HW-1K-F1”, “MCR-HW-5K-F1”, “MCR-HW-10K-F1”, “MM-HW-1K-F1”, “MM-HW-5K-F1”, “MM-HW-10K-F1”, “Intel Xeon E5”, “Linux OS Kernel”, “Aruba OpenSSH”, “Aruba SSH”, “Aruba OpenSSL”, “Aruba SSL”, “Aruba TLS”, “Mocana Cryptographic Library”, “Mocana”, “Aruba Crypto Module”, “Aruba Bootloader Module”, “AOS”, “OpenSSL”, “OpenSSH”, and “sos”.

The Evaluation team conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

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.

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 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, performed the Assurance Activities in the NDcPP30e/SSH10, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the instructions in the Guidance documents defined in Section 6. No other versions of the TOE and software, either earlier or later, were evaluated.

The evaluated functionality is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionalities provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

Per NIAP/CCEVS Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0 Security Target,* Version 1.0, October 15, 2026.

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 3.0e, 06 December 2023 (NDcPP30e).

[5] *Functional Package for SSH*, Version 1.0, 13 May 2021 (SSH10).

[6] *HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0 Security Target*, Version 1.0, October 15, 2026 (ST).

[7] *Assurance Activity Report for HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0*, Version 0.3, October 15, 2026 (AAR).

[8] *Detailed Test Report for HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0*, Version 0.3, October 15, 2026 (DTR).

[9] *Evaluation Technical Report for HPE Networking Hardware Mobility Conductor Series running HPE Aruba Networking Wireless Operating System 8.13.0*, Version 0.3, October 15, 2026 (ETR).

[10] *HPE Aruba Networking Wireless Operating System 8.13.0 Supplemental Guidance (Common Criteria Configuration Guidance)*, Version 3.2, October 2026 (AGD).