National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11

Report Number: CCEVS-VR-VID11404-2023
Dated: October 21, 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

Swapna Katikaneni
Fernando Guzman
Jerome F Myers

Common Criteria Testing Laboratory

Cornelius Haley
Dip Pudasaini
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 Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11solution provided by Alcatel-Lucent Enterprise. 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 October 2023. 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 2.2e, 23 March 2020.

The Target of Evaluation (TOE) is the Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11.

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 Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11 Security Target, version 0.7, October 9, 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 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	Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020
ST	Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11 Security Target, version 0.7, October 9, 2023
Evaluation Technical Report	Evaluation Technical Report for Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11, version 0.2, October 9, 2023
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	ALE USA Inc
Developer	Alcatel-Lucent Enterprise
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Swapna Katikaneni, Jerome F Myers, Fernando Guzman

3 Architectural Information

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

The Target of Evaluation (TOE) is the Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, and 9900 with AOS 8.9 R11. The firmware is named Alcatel-Lucent Operating System (AOS) which is the single purpose operating system that operates the management functions of all of the Alcatel-Lucent Enterprise OmniSwitch switches.

3.1 TOE Description

The TOE provides Layer-2 switching, Layer-3 routing, and traffic filtering. Layer-2 switching analyzes incoming frames and makes forwarding decisions based on information contained in the frames. Layer-3 routing determines the next network point to which a packet should be forwarded toward its destination. These devices may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet. Routing protocols include Border Gateway Protocol (BGP), Routing Information Protocol (RIP) v.2, and Open Shortest Path First (OSPF). Filtering controls network traffic by controlling whether packets are forwarded or blocked at the TOE's interfaces. Each packet is examined to determine whether to forward or drop the packet, on the basis of the criteria specified within the access lists. Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

All series perform the same security functions with respect to this evaluation. The differences between the models are in speed and physical characteristics.

The intended TOE environment is a secure data center that protects the TOE from unauthorized physical access. Only security administrators are to have access to connect to the serial console, or gain physical access to the hardware. Appropriate administrator security policy and security procedure guidance must be in place to govern operational management of the TOE within its operational environment.

The TOE is not intended for use as a general purpose computer and only executes the services needed to perform its intended function.

3.2 TOE Evaluated Platforms

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

3.3 TOE Architecture

Each TOE appliance runs the AOS 8.9 R11 software and has physical network connections to its environment to facilitate managing and filtering network traffic.

3.4 Physical Boundaries

The TOE is located between the external and the internal network or within the internal network of an organization in order to perform Layer-2 switching, Layer-3 routing, and traffic filtering of flowing IP packets. TOE audit records can be optionally stored in a Syslog Server. Communication is protected by the TLS protocol.

Administrators log onto the TOE and perform management functions via a Command Line Interface (CLI). These activities can be performed via a Serial Console connected to the TOE via a dedicated port, or using an SSHv2 client from a computer connected to the security management network. Administrators can execute commands from the CLI to connect to external SSH via the SSHv2 protocol.

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 generates audit records. The audit records can be displayed on the serial console as they are generated in a scrolling format.

The TOE writes audit records to a set of circular files stored in the systems flash memory for permanent storage. These entries are tagged with the AOS application ID of the TOE subsystem that triggers the audit records to be generated. The TOE also provides the ability to send the audit records to an external syslog server using a secure channel.

The TOE provides to security administrators the ability to modify the maximum size allowed for the audit files. Once the files are full the oldest entries are overwritten.

4.2 Cryptographic support

The TOE requires cryptography for supporting the following functionality.

- Establishment of secure channels using the SSHv2 and TLSv1.2 protocols
- X.509 certificate generation and validation
- Storage of passwords
- Self-tests of the cryptographic algorithms
- Verification of the integrity of the TOE firmware

The TOE provides cryptographic support using the OpenSSL and OpenSSH software packages, which are bundled in the TOE.

4.3 Identification and authentication

The TOE requires identification and authentication of administrators of the TOE prior to access any of the management functionality in all possible scenarios, which are as follows.

- TOE administrators accessing (either locally or remotely) the Command Line Interface (CLI) via a serial console or a Secure Shell (SSH) session

The TOE displays to the administrator a configurable banner before the administrator successfully logs onto the TOE (either serial console or SSH). The TOE also provides the ability to lock the administrator after a configurable number of unsuccessful attempts, and terminate the logon session after a configurable period of inactivity.

The TOE provides administrator configurable password settings to enforce password complexity when a password is created or modified.

The TOE provides support for the following Identification and Authentication mechanisms.

- Identification and Authentication made by the TOE using credentials stored in the local file system
- Communication with SSH clients is protected with the Secure Shell (SSH) protocol.

4.4 Security management

The TOE provides a Command-Line Interface (CLI) for security management. TOE administrators connect to the TOE via either a serial console or a remote session using Secure Shell (SSHv2). In either case, administrators are required to identify and authenticate against the TOE before getting access to the CLI.

4.5 Protection of the TSF

The TOE protects itself by requiring administrators to identify and authenticate themselves prior to performing any actions and by defining the access allowed by each administrator. The TOE uses the filesystem access control to protect access to sensitive data like cryptographic keys and credentials.

The TOE ensures that manual updates of the TOE firmware are done using trusted updates by verifying the integrity of the new version of the TOE firmware.

The TOE also implements self-tests to ensure the correct operation of cryptographic services.

The TOE also provides a reliable date and time that is used for audit record timestamps, certificate verification and session timing.

4.6 TOE access

The TOE can be configured to display a login banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

4.7 Trusted path/channels

The TOE provides the following secure channels to ensure the integrity and confidentiality of the information exchanged between the TOE and external IT entities in the operational environment.

- Transport Layer Security (TLS) versions 1.2 is used to protect communication with external audit servers (syslog).
- Secure Shell version 2 (SSHv2) is used to protect communication with SSH clients.

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

That information has not been reproduced here and the NDcPP22e 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 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 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 Network Device 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 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:

- Preparation and Operation of Common Criteria Evaluated OmniSwitch Products (NDcPP), AOS Release 8.9.R11, July 2023

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 Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11, Version 0.2, October 9, 2023 (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 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices and section 3.4 provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The TOE hardware consists of the following OminSwitch models when configured in accordance with the documentation specified in Section 6 of this report :

Model	Processor ID	Microarchitecture	Network Interface
OmniSwitch 6360 (OS6360)	Marvell 98DX236S	ARM Cortex-A9	Marvell AlleyCat 3
	Marvell 98DX233S	ARM Cortex-A9	Marvell AlleyCat 3
OmniSwitch 6465 (OS6465/OS6465T)	Marvell 98DX3233	ARM Cortex-A9	Marvell AlleyCat 3
OmniSwitch 6560 (OS6560)	Marvell 88F6820	ARM Cortex-A9	Marvell AlleyCat 3
OmniSwitch 6860 (OS6860E)	Broadcom BCM56342	ARM Cortex-A9	Broadcom Helix4
	Broadcom BCM56340	ARM Cortex-A9	Broadcom Helix4
OmniSwitch 6860 (OS6860N)	Intel Atom C3338	Goldmont	Broadcom Trident3
	Intel Atom C3558	Goldmont	Broadcom Trident3
OmniSwitch 6865 (OS6865)	Broadcom BCM56342	ARM Cortex-A9	Broadcom Helix4
OmniSwitch 6900 (OS6900)	Intel Atom C3558	Goldmont	Broadcom Trident3
	Intel Atom C2538	Rangeley	Broadcom Tomahawk
	Intel Xeon D1518	Broadwell	Broadcom Trident3
OmniSwitch 9900 (OS9900)	Intel Atom C2518	Rangeley	Marvell Prestera DX

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 Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

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 Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11 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 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 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. The public search for vulnerabilities did not uncover any residual vulnerability.

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

The search was performed on October 9, 2023. The search was conducted with the following search terms: "Alcatel-Lucent", "OminSwitch", "SSH", "TLS", "ARM Cortex A9", "Intel Atom C3558", "Intel Atom C2338", “OpenSSL 3.0.7”. Intel Atom C2538”, “Intel Xeon D1518”, “Intel Atom C2518”, “Marvell 98DX236S”, “Marvell 98DX233S”, “Marvell 88F6820”, “Broadcom BCM56342”, “Broadcom BCM56340”.

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

As stated in section 5, the scope of this evaluation was limited to the functionality and assurances covered in the collaborative Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E]. 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. The evaluated configuration is dependent upon the TOE being configured per the evaluated configuration described in section 8 and the instructions in the Administrator Guide document listed in section 6.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11 Security Target, Version 0.7, October 9, 2023*.

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.

[5] Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9 R11 Security Target, Version 0.7, October 9, 2023 (ST).

[6] Assurance Activity Report for Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9.R11, Version 0.2, October 9, 2023 (AAR).

[7] Detailed Test Report for Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9.R11, Version 0.2, October 9, 2023 (DTR).

[8] Evaluation Technical Report for Alcatel-Lucent Enterprise OmniSwitch series 6360, 6465, 6560, 6860, 6865, 6900, 9900 with AOS 8.9.R11, Version 0.2, October 9, 2023 (ETR)