National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms

Version 1.0

Report Number: CCEVS-VR-VID11400-2024

Dated: 03/12/2024

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

Lauren Brandt

Jenn Dotson

Sheldon Durrant

Clare Parran

Lisa Mitchell

Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Kamran Farogh

Rupendra Kadtan

Joan Marshall

Fathi Nasraoui

Shaunak Shah

Acumen Security, LLC

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of the Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms provided by Ciena Corporation. 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 of the TOE is either expressed or implied.

The evaluation was performed by the Acumen Security Common Criteria Testing Laboratory (CCTL) in Rockville, MD and completed in March 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the *collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 [NDcPPv2.2e]*.

The TOE is the Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms 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 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 *Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms Security Target*, v1.3, 11 March 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 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	Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
Security Target	*Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms Security Target*, v1.3, 11 March 2024
Evaluation Technical Report	*Evaluation Technical Report for SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms*, v0.8, 11 March 2024
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Ciena Corporation
Developer	Ciena Corporation
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd Suite 395 Rockville, MD 20850
CCEVS Validators	Lauren Brandt, Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Clare Parran, Lori Sarem

3 Architectural Information

3.1 TOE Overview

The TOE is the Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms. It is a non-distributed, non-virtual network device which implements routing and switching functionalities for enterprise, mobility, and converged network architectures. In these architectures, the TOE can be deployed in the access, aggregation, or core of the network. The TOE uses a Linux based container architecture for its SAOS Network Operating System and includes the Ciena SAOS 10.7.1 operating system executed on the Ciena 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms.

3.2 TOE Evaluated Configuration

The TOE is the SAOS 10.7.1 executed on the 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms summarized in the following table. The same software is executed on each platform.

Table 1 TOE Hardware Platforms

Models/Platform	1G/10G SFP+	Processors	100G	Power Options
3926	6	4x1.5GHz ARM Cortex A53	--	AC, DC
3928	4	4x1.5 GHz ARM Cortex A53	--	AC, DC
3948	4	4x1.5 GHz ARM Cortex A53	--	AC, DC
5144	8	4x2GHz ARM Cortex A72	--	AC, DC
5164	32x[1G/10G/25G]	4x2GHz ARM Cortex A72	4x [100G/ 200G]	AC, DC
5162	40	Intel XEON D1527, 4CORE	2	AC, DC
5170	4x 25G/10G/1G and 36x 10G/1G	Intel XEON D1527, 4CORE	4xQSFP28	AC, DC
8180	--	Intel XEON D1527, 4CORE	32xQSFP28 FRU module options: 1xWLAi FRU and 4x100G CFP2-DCO	AC, DC
5171	4x 25G/10G/1G and 36x 10G/1G	Intel XEON D1539, 8CORE	FRU module options: 2x QSFP28, 1x QSFP28 + 1x 100G CFP2-DCO, 2x 100G CFP2-DCO, 1x200G CFP2-DCO	AC, DC
Large NFV compute server (FRU)	--	Intel XEON D1548, 8CORE	--	--

3.3 Physical Scope of the TOE

The TOE is deployed in an environment that includes the IT components illustrated in Figure 1. The physical boundary of the TOE is also illustrated in Figure 1. The TOE itself is delivered as an appliance or an FRU with the software installed.

The environmental components described in Table 2 are required to operate the TOE in the evaluated configuration. The TOE implements a TLS Client and SSH Server for secure connectivity to the components of the environment. Each component of the environment is required to implement the corresponding client and/or server. The remote management workstation is required to implement a SSH

Client for accessing the TOE, and the audit server, and file server must include a TLS Server for which the TOE can connect using the TLS Client. Communication with the file server is via HTTPS/TLS.

Figure 1: TOE Boundary and Operational Environment

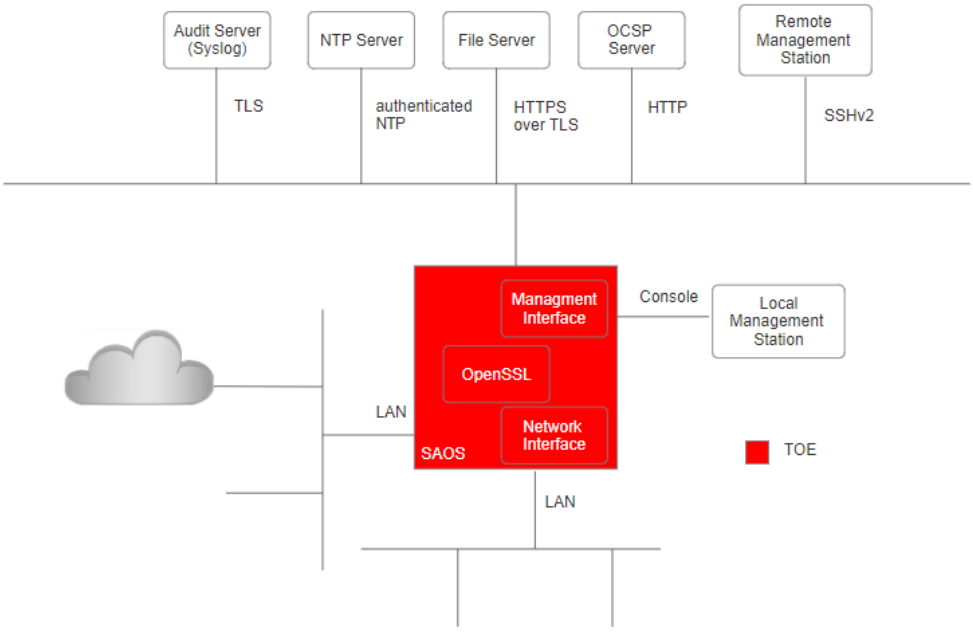

Table 2 Environmental Components of the TOE

Component	Purpose/Description
Audit server	The audit server supports syslog messages over TLS to receive the audit files from the TOE. The audit data is stored in the remote audit server for redundancy purposes.
NTP server	An external NTP Server for synchronizing the TOE time with. NTP time stamps are protected from tampering using SHA-1 for authentication.
File Server	Remote file server for storing user files and updating the TOE. Communication with the File Server is with HTTPS over TLS.
OCSP Server	Validity of the certificates the TOE uses for asserting the authenticity of the TLS peers is verified using OCSP. Communication with an OCSP Server is over HTTP.
Management Workstation	A workstation used by an administrator to manage the TOE locally or remotely. The remote management station must include a SSHv2 client.

3.4 Excluded Functionality

The following product functionality is not covered by the evaluation:

- Telnet is not included and must be disabled.
- Telemetry Client must not be used.
- MACsec functionality is not evaluated and must not be used.
- SNMP is not evaluated and must be disabled.
- FTP to upload or download files/configuration is not evaluated and must be disabled.

4 Security Policy

This section summarizes the security functionality of the TOE.

4.1 Security Audit

The TOE implements extensive auditing capabilities to allow legitimate administrators to examine the events that have occurred. Audit records are generated for all auditable events, including the starting and stopping of the audit service and each auditable event stated in ST. The TOE stores audit records locally and may be configured to export them to an external audit server using syslog over TLS. Each audit record contains the date and time of event, type of event, subject identity, and any other event-related relevant data.

4.2 Cryptographic Support

The TOE includes the OpenSSL v3.0.8 library which implements cryptographic functions and protocols for trusted paths and trusted channels. Specifically, the TOE implements an SSH server and a TLS client for communication with trusted peer entities. Peer entity authentication for TLS is using X.509 public key certificates. Cryptographic algorithms are all Cryptographic Algorithm Validation Program (CAVP) validated. The validation certificate references are given in ST.

TLS v1.2 is used for protecting the transfer of syslog messages to an external Syslog server.

HTTPS over TLS is used for secure transfer of files to an external File Server.

SSH is used to protect the remote management of the TOE. Remote management of the TOE is using CLI over SSH.

4.3 Identification and Authentication

The TOE authenticates all users connecting to the management interfaces of the TOE. Authentication may take place over the console for local access or over SSH for remote access. Only upon successful authentication, given that the user is authorized for the role, is a user assigned to the role administrator and granted access to the management functions of the TOE. Local users authenticate to the TOE using a username and password. Remote users may also use SSH public-key authentication. A customizable warning banner is displayed at each authentication window.

The TOE uses X.509v3 certificates for peer entity authentication of TLS peers. The TSF determines the validity of the certificates by confirming the validity of the certificate chain and verifying that the certificate chain ends in a trusted Certificate Authority (CA). The TOE connects to an Online Certificate Status Protocol (OCSP) server using HTTP (unsecure) to confirm the revocation status of the certificates.

4.4 Security Management

The TOE allows local and remote management of its security functions. Local management is from a management workstation connected to the console or USB port of the TOE and the remote management is from a workstation connected to the TOE over SSHv2.

All management functions are implemented using the CLI and are only made available to authorized administrators upon successful identification and authentication. There are no other management interfaces than the CLI, i.e., the CLI implements each management function of the TOE.

The management functions the TOE implements include the ability to configure the access banner the TOE displays at each authentication window, the ability to configure the session inactivity timers, the ability to update the TOE software and to verify the authenticity of the updates, the ability to configure the authentication failure parameters, the ability to configure audit behavior, the ability to modify the behavior of the transmission of audit data to an external syslog server, the ability to manage the cryptographic keys, the ability to configure thresholds for SSH rekeying, the ability to set the time which is used for time-stamps, the ability to configure Network Time Protocol (NTP), the ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors, and the ability to import X.509v3 certificates to the TOE's trust store.

4.5 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys, and private keys from unauthorized disclosure. Pre-shared keys, symmetric keys, and private keys are stored encrypted. An exception is the SSH host keys which are required by the SSH Daemon when the SSH starts. The SSH Daemon is executed at the root privileges and the SSH host keys are only accessible with root privileges. No user of the TOE is granted root privileges. Passwords are stored as non-reversible hash values computed using SHA-512 using the Linux Pluggable Authentication Module (PAM) functions. The TOE maintains system time via its local hardware clock which is manually set by an administrator. The administrator may also configure the TOE to connect to an NTP server for time synchronization.

The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE and verify the authenticity of all updates prior to the installation.

Access to the TOE functions is only using the CLI from the management ports. The CLI cannot be invoked from the ports used for connecting the subnetworks across the TOE. Access to the CLI is only granted to authorized administrators upon successful authentication.

4.6 TOE Access

Prior to establishing an administration session with the TOE, an access banner is displayed to the user. The banner messaging is customizable but is typically used to warn the users of the consequences of attempted unauthorized access. The TOE will terminate an interactive session after a configurable time of session inactivity. A user may terminate his/her local and remote administrative sessions on will. Users may change their own passwords, but the TOE enforces minimum quality criteria for the passwords. The TOE also maintains a counter for consecutive failed authentication attempts for each user. If the counter value reaches an administrator-defined threshold, the TOE triggers protective measures to prevent password guessing attacks.

4.7 Trusted path/Channels

The TOE implements trusted paths and trusted channels. The trusted path is a SSH connection between the TOE and the remote management workstation. The SSH client of the remote management workstation connects to the SSH Server implemented by the TOE. Upon successful connection establishment and authentication of the user, the remote administrator uses the CLI over SSH to manage the TOE.

For trusted channels, the TOE implements a TLS client used by the TOE to connect to the peer entities. The peer entities are a remote File server and the syslog server. Both systems are mandatory in the

Operational Environment. The TOE also implements HTTPS over TLS for connecting to a remote file server. The TLS Client is only used for TLSv1.2 connections.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the *collaborative Protection Profile for Network Devices*, v2.2e, 23 March 2020 (NDcPPv2.2e)

That information has not been reproduced here and the NDcPPv2.2e 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 NDcPPv2.2e 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 NDcPPv2.2e and performed by the Evaluation team.
- This evaluation covers only the specific software version identified in this document and referenced in the *Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms Security Target*, v1.3, 11 March 2024, 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 NDcPPv2.2e 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 provided with the TOE for evaluation:

- *Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms CC Guidance Supplement*, v1.3, 11 March 2024
- *3948/513x/5144/516x/5170/811x Routers and Platforms, Security SAOS 10.7.1*, May 2022
- *5162 Router, Installation*, November 2023
- *D-NFVI Software, D-NFVI Installation, D-NFVI 10.7.1*, May 2022

7 IT Product Testing

This section describes the testing efforts of the Evaluation team. It is derived from information contained in the ETR and Detailed Test Reports (DTRs) for Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms, which are not publicly available. The Assurance Activity Report (AAR) provides an overview of testing and the prescribed assurance activities.

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 verified the product according to the vendor-provided guidance documentation and ran the tests specified in the *Evaluation Activities for Network Device cPP, Version 2.2e*, December-2019 [NDcPPv2.2e SD]. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target. The Evaluation team used the NDcPPv2.2e SD test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

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 documents: the DTR and the ETR. The reader of this document can assume that 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 NDcPPv2.2e SD.

The Evaluation determined the TOE satisfies the conformance claims made in the *Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms Security Target*, v1.3, 11 March 2024 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

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 Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms 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

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 Evaluation team 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

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

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

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 Test Reports, 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

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Vulnerability Assessment for the TOE: Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms*, v0.7, March 11, 2024, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities, last conducted on February 29, 2024, did not uncover any residual vulnerabilities.

The Evaluation team searched:

- https://nvd.nist.gov/vuln/search
- http://cve.mitre.org/cve
- https://www.cvedetails.com/vulnerability-search.php
- https://www.kb.cert.org/vuls/search/
- www.exploitsearch.net
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories
- https://www.exploit-db.com
- https://www.rapid7.com/db/vulnerabilities
- https://www.ciena.com/

The Evaluation team's search used the following keywords:

- Ciena Switch
- Ciena Router
- Ciena SAOS
- Ciena SAOS 10.7.1

- Ciena 3926
- Ciena 5162
- Ciena 3928
- Ciena 3948
- Ciena 5144
- Ciena 5164
- Ciena 5170
- Ciena 5171
- Ciena 8180
- Ciena
- SAOS 10.7.1
- Intel XEON D1527
- Intel XEON D1539
- Intel XEON D1548
- ARM Cortex A72
- ARM Cortex A53
- OpenSSL 3.0.8
- OpenSSH 8.4
- Linux kernel 5.4.154
- Infineon SLM9670
- Infineon SLB9665
- SAOS
- Large NFV Compute Server
- Linux Pluggable Authentication Module
- tls v1.2
- rsyslogd 8.1903.0
- ntp 4.2.8p15

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 NDcPPv2.2e SD, and correctly verified that the product meets the claims in the ST.

9 Validator Comments & Recommendations

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.

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in *Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms CC Guidance Supplement*. 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

Ciena SAOS R10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms Security Target, v1.3, 11 March 2024

12 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.

13 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.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. *Collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 [NDcPPv2.2e].
6. *Evaluation Activities for Network Device cPP, Version 2.2e*, December-2019 [NDcPPv2.2e SD]
7. *Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms Security Target*, v1.3, 11 March 2024 [ST]
8. *Ciena SAOS 10.7.1 on the 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms CC Guidance Supplement*, v1.3, 11 March 2024 [AGD]
9. *Assurance Activity Report for Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms*, v0.8, March 11, 2024 [AAR]
10. *Evaluation Technical Report for Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms*, v0.8, 11 March 2024 [ETR]
11. *Test Plan for Ciena 3926 SAOS 10.7.1*, v0.4, 11 March 2024 [DTR]
12. *Test Plan for Ciena 5162 SAOS 10.7.1*, v0.4, 11 March 2024 [DTR]
13. *Vulnerability Assessment for the TOE: Ciena SAOS 10.7.1 on 3926, 3928, 3948, 5144, 5162, 5164, 5170, 5171, Large NFV Compute Server, and 8180 Service Aggregation Platforms*, v0.7, March 11, 2024 [AVA]
14. *3948/513x/5144/516x/5170/811x Routers and Platforms, Security SAOS 10.7.1*, May 2022
15. *5162 Router, Installation*, November 2023
16. D-*NFVI Software, D-NFVI Installation, D-NFVI 10.7.1*, May 2022