# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme


TM

# Validation Report

# for the

# Ciena Waveserver Ai Rel 1.3

**Report Number:** CCEVS-VR-VID10967-2019

**Dated:** June 26, 2019

**Version:** 1.4

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

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6940**
**Fort Meade, MD 20755-6940**

# ACKNOWLEDGEMENTS


## Validation Team

Paul Bicknell

Michelle Carlson

Lisa Mitchell

Linda Morrison

Patrick Mallett, PhD

Clare Olin

Jean E Petty

*MITRE Corporation*

## Common Criteria Testing Laboratory

Dayanandini Pathmanathan

Natasha Mathias

Scott Ehrlich

*Acumen Security, LLC*

# Table of Contents

# 1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Ciena Waveserver Ai Rel 1.3 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in June 2019. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, 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 U.S. Government Protection Profile for Security Requirements for collaborative Protection Profile for Network Devices + Errata 20180314, Version 2.0e.

The Target of Evaluation (TOE) identified in this VR 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), as interpreted by the Assurance Activities contained in the NDcPP v2.0e. 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 provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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.

# 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Product Compliance 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, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) 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 Waveserver Ai Rel 1.3 |
| **Protection Profile** | collaborative Protection Profile for Network Devices + Errata 20180314, Version 2.0e |
| **Security Target** | Ciena Waveserver Ai Rel 1.3 Security Target v2.6, June 14, 2019 |
| **Evaluation Technical Report** | Ciena Waveserver Ai Rel 1.3 Evaluation Technical Report, Version 1.9, June 19, 2019 |
| **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 |
| **CCEVS Validators** | Patrick W Mallett, Michelle Carlson, Paul Bicknell, Linda Morrison, Lisa Michelle, Jean E Petty |

# 3 Architectural Information

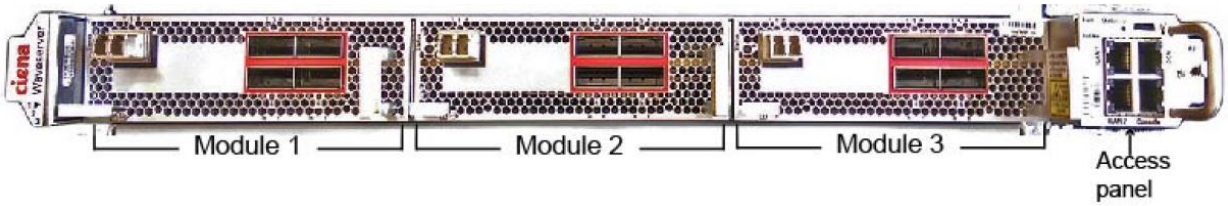
The Ciena Waveserver (herein referred to as the TOE) Ai Rel 1.3 is a network device which offers ultra-high capacity connections between data center locations thus reducing the network costs for both enterprises and content providers. The Wavesever Ai utilizes the Ciena's WaveLogic Ai technology. The Waveserver Ai uses the WCS2 hardware.

Waveserver Ai features a modular design that accommodates up to three Waveserver Ai traffic modules supporting a range of client capacities, speeds, bands and pluggables. The TOE hardware is comprised of the following:

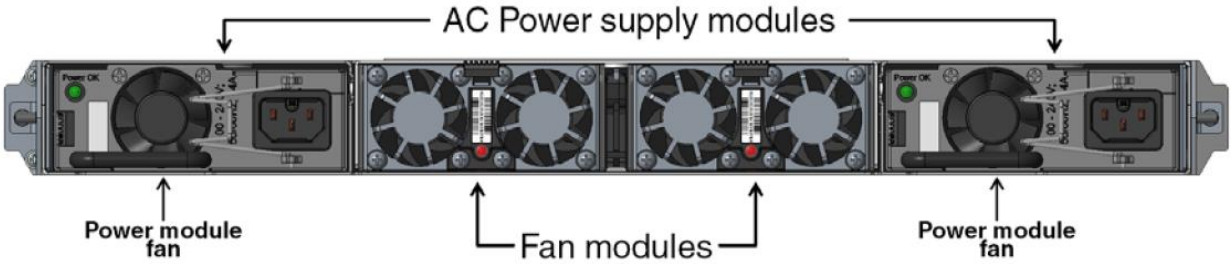
- Number of traffic module slots: 3
- Control module: 1 (WCS2)
- Access panel: 1
- Cooling: 2 fans
- Power units: 2
- Power options: AC, DC

**Figure 1 Front and Rear Panels for the TOE**

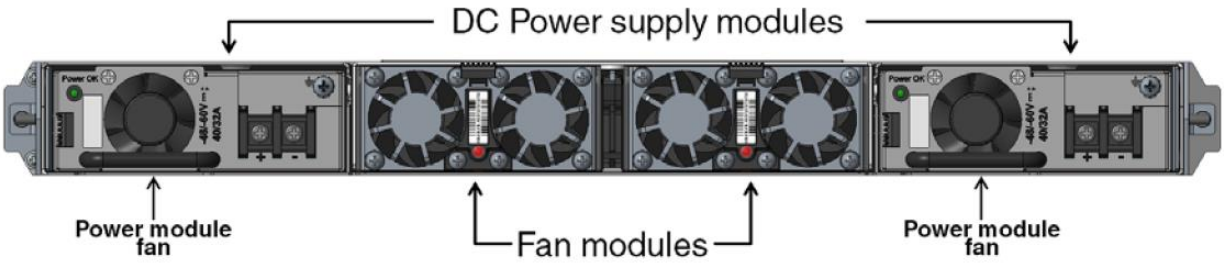
Waveserver Ai front panel:




Waveserver Ai rear panel: AC power and fan modules



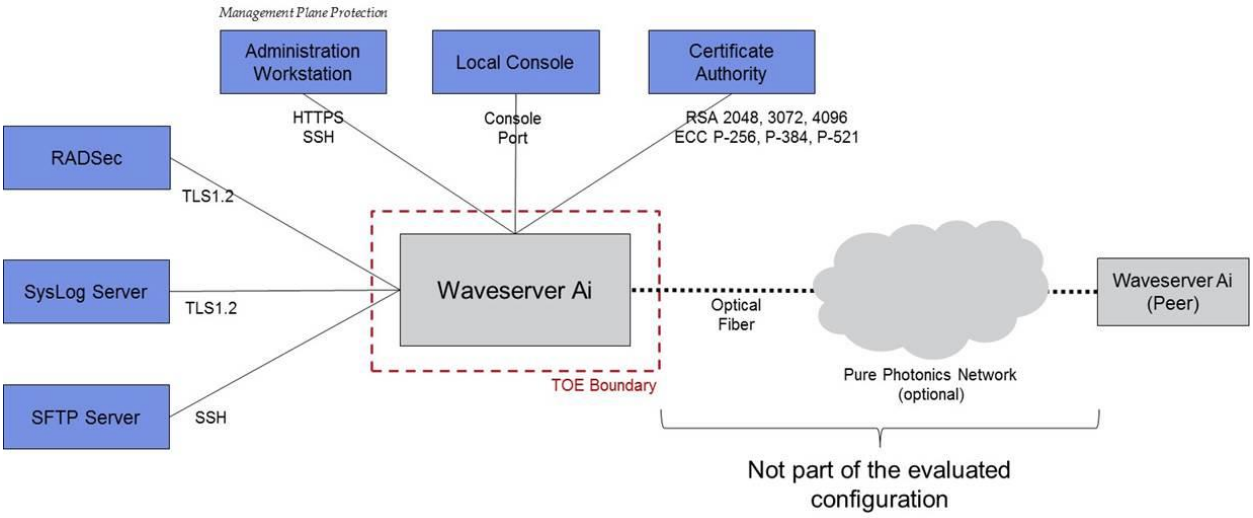

Waveserver Ai rear panel: DC power and fan modules



The TOE resides on a network and supports (in some cases optionally) the following hardware, software and firmware in its environment.

- Administration Workstation: Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed locally with the console port connection or remotely with HTTPS or SSH connection. *NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested.*
- SysLog Server: A general-purpose computer that is running a TLS SysLog server, which is used to store audit data generated by the TOE.
- RADSec Server: A general-purpose computer that is running a RADIUS over TLS server, which is used for user authentication by the TOE.
- SFTP Server: A server running the secure file transfer protocol (SFTP) that is used as a location for storing product updates that can be transferred to the TOE.
- Certificate Authority: Certificate Authority is used for creation and management of X509 certificates to be used with the TOE. It can also be used to validate a certificate's revocation status with Online Certificate Status Protocol (OCSP).

**Figure 2 TOE Deployment**



# 4 Security Features

The TOE implements the following security functional requirements:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

Each of these security functionalities are listed in more detail below.

**Security Audit**

The TOE generates audit events for all start-up and shut-down functions, and all auditable events. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE is capable of storing audit events locally and exporting them to an external syslog server using TLS v1.2 protocol. Each audit record contains the date and time of event, type of event, subject identity, and the relevant data of the event. The syslog server supports the following severity levels: emergency, alert, error, warning, notice, info and debug. In order to enable the logging to syslog server, a user must be logged in with an administrative access privilege.

**Cryptographic Support**

The TOE provides cryptographic support for the services described in Table 1. The related CAVP validation details are provided in Table 2. The operating system is Linux Kernel v4.9. The TOE leverages the Waveserver Ai WCS-2 FW Crypto Library 2 for its cryptographic functionality. .

| Cryptographic Method | Usage |
|---|---|
| FCS_CKM.1 Cryptographic Key Generation | Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS), Appendix B.3.<br>RSA Key sizes supported are 3072 and 4096 bits. 4096 bits support was not tested/evaluated.<br>RSA key size of 2048 bits must be enabled in the evaluated configuration<br>Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS)", Appendix B.4<br>Elliptic NIST curves supported are: P-256, P-384 and P-521. |
| FCS_CKM.2 Cryptographic Key Establishment | RSA-based key establishment conforming to RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 |

| | |
|---|---|
| | Elliptical curve based establishment conforming to NIST Special Publication 800-56A Revision 2.<br>Key establishment using Diffie-Hellman group 14 conforming to RFC 3526, Section 3. |
| FCS_CKM.4 Cryptographic Key Destruction | The TOE satisfies key zeroization. |
| FCS_COP.1/DataEncryption | AES encryption and decryption conforming to CBC as specified in ISO 10116, CTR as specified in ISO 10116 and GCM as specified in ISO 19772.<br>AES key size supported is 256 bits<br>AES modes supported are: CBC, CTR and GCM. |
| FCS_COP.1/SigGen | RSA digital signature algorithm conforming to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3.<br>RSA key size of 2048 bits must be enabled in the evaluated configuration<br>RSA key sizes supported are: 3072 and 4096 bits. 4096 bits support was not tested/evaluated.<br>Elliptical curve digital signature algorithm conforming to FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" ISO/IEC 14888-3, Section 6.4.<br>Elliptical curve key size supported is 256 bits. |
| FCS_COP.1/Hash | Cryptographic hashing services conforming to ISO/IEC 10118-3:2004.<br>Hashing algorithms supported are: SHA-256, SHA-384 and SHA-512.<br>Message digest sizes supported are: 256, 384 and 512 bits. |
| FCS_COP.1/KeyedHash | Keyed-hash message authentication conforming to ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm.<br>Keyed hash algorithm supported are: HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512.<br>Key sizes supported are: 256, 384, and 512 bits.<br>Message digest sizes supported are: 256, 384 and 512 bits. |
| FCS_DRBG_EXT.1 Random Bit Generation | Random number generation conforming to ISO/IEC 18031:2011.<br>The TOE leverages CTR_DRBG(AES)<br>CTR_DRBG seeded with HW_TRNG with a minimum of 256 bits of entropy. |
| FCS_HTTPS_EXT.1 HTTPS Protocol | The TOE supports HTTPS protocol that complies with RFC2818.<br>The TOE implements HTTPS protocol using TLS v1.2 in support of Web UI. |

| | |
|---|---|
| FCS_TLSC_EXT.2 TLS Client Protocol with authentication | The TOE supports TLS v1.2 protocol for use with X. 509v3 based authentication.<br>Supports the following ciphersuites in the evaluated configuration:<br><br>TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246<br>TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC<br>5288TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289<br>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289<br>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289<br>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 |
| FCS_TLSS_EXT.2 TLS Server Protocol with mutual authentication | The TOE supports TLS v1.2 protocol and supports mutual authentication for use with X.509v3 certificates.<br>Supports the following ciphersuites in the evaluated configuration:<br><br>TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246<br>TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC<br>5288TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289<br>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289<br>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289<br>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 |
| FCS_SSHS_EXT.1 SSH Server Protocol | The TOE supports SSH v2 protocol.<br>Supports password-based authentication.<br>SSH public-key authentication uses rsa-ssh, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521.<br>SSH transport uses the following encryption algorithms: AES256-CTR and AEAD_AES_256_GCM.<br>Packets greater than 256 000 bytes in an SSH transport connection are dropped. |

| | |
|---|---|
| | SSH transport uses the following data integrity MAC algorithms: hmac-sha2-256, and hmac-sha2-512 and AEAD_AES_256_GCM.<br>Key exchange algorithms supported are: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521.<br>The TOE ensures that within SSH connections the same session keys are used for a threshold of no longer than one hour and no more than 512 MB of transmitted data. |

**Table 1 TOE Cryptography Implementation**

| Cryptographic Algorithms | CAVPs |
|---|---|
| AES | C193 |
| RSA | C193 |
| ECDSA | C193 |
| KAS/CVL | C193 |
| HMAC | C193 |
| SHS | C193 |
| DRBG | C193 |
| CVL SSH v2 | C193 |
| CVL TLS v1.2 | C193 |

**Table 2 Cryptographic Algorithm Certificates**

**Identification and Authentication**

The TOE supports Role Based Access Control. All users must be authenticated to the TOE prior to carrying out any management actions. The TOE supports password-based authentication and public key based authentication. Based on the assigned role, a user is granted a set of privileges to access the system.

**Security Management**

The TOE supports local and remote management of its security functions including:

o Local console CLI administration
o Remote CLI administration via SSHv2
o Timed user lockout after multiple failed authentication attempts
o Password configurations.
o Role Based Access Control – Superuser (Security Administrator), Admin and limited user (User)
o Configurable banners to be displayed at login
o Timeouts to terminate administrative sessions after a set period of inactivity
o Protection of secret keys and passwords

**TOE Access**

Prior to establishing an administration session with the TOE, a banner is displayed to the user. The banner messaging is customizable. The TOE will terminate an interactive session after 10 minutes of session inactivity. An administrator can terminate their GUI session by clicking on the logout button. A user can terminate their local CLI session and remote CLI session by entering exit at the prompt.

**Protection of the TSF**

The TOE protects all passwords, pre-shared keys, symmetric keys and private keys from unauthorized disclosure. Passwords are stored in encrypted format. Passwords are stored as SHA-512 salted hash value as per standard Linux approach. 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. The TOE internally maintains the date and time.

**Trusted Path/Channels**

The TOE supports TLS v 1.2 for secure communication to the following IT entities: Syslog server and Radius server. The TOE supports HTTPS/TLS (WebUI ) and SSH v2 (remote CLI) for secure remote administration.

*NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested.*

# 5 Assumptions, Threats & Clarification of Scope

## 5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

A.PHYSICAL_PROTECTION

The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. [OE.PHYSICAL]

A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking functionality). [OE.NO_GENERAL_PURPOSE]

A.NO_THRU_TRAFFIC_PROTECTION

A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall). [OE.NO_THRU_TRAFFIC_PROTECTION]

A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device. [OE.TRUSTED_ADMIN]

A.REGULAR_UPDATES

The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities. [OE.UPDATES]

A.ADMIN_CREDENTIALS_SECURE

The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside. [OE.ADMIN_CREDENTIALS_SECURE]

A.RESIDUAL_INFORMATION

The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

## 5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a

loss of confidentiality and integrity, and potentially the network device itself could be compromised.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.

T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.

T.PASSWORD_CRACKING

Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other network devices.

T.SECURITY_FUNCTIONALITY_FAILURE

An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

### 5.3 Clarification of Scope

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, with a certain level of assurance. The level of assurance for this evaluation is defined within the NDcPP.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

# 6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Ciena Waveserver Ai Rel 1.3 Security Target, v2.6, June 14, 2019
- Ciena Waveserver Ai Rel 1.3 Common Criteria Guidance Document, v1.1, June 19, 2019.

# 7 TOE Evaluated Configuration

## 7.1 Evaluated Configuration

The TOE in the evaluated configuration consists of theWaveserver Ai Rel 1.3.

The TOE supports secure connectivity with other IT environment device as stated in Table 3.

**Table 3 IT Components**

| Component | Required | Usage |
|---|---|---|
| NTP server (optional) | No | The TOE supports communication with an NTP server to synchronize date and time. |
| Syslog server | Yes | The TOE exports audit events to an external syslog server via TLS v1.2 protocol. |
| Radius server | Yes | The TOE supports secure communication to RADIUS server via TLS v1.2 protocol. |
| Management workstation with Web Browser/SSH client | Yes | This includes any IT Environment Management workstation with a Web Browser and a SSH client installed that is used by the TOE.<br><br>*NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested.* |
| Certificate Authority server | Yes | The Certificate Authority is used for creation and management of X509 certificates to be used with the TOE. |

## 7.2 Excluded Functionality

The following interfaces are not included as part of the evaluated configuration:

- NTP server (optional)
- The Web UI management interface is out of scope (All HTTPS and TLSS requirements were evaluated and tested)
- gRPC is disabled

# 8 IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in Evaluation Test Report for Ciena Waveserver Ai Rel 1.3, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

## 8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

## 8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

All testing was carried out at the Ciena Corporation offices located in 385 Terry Fox Dr, Ottawa, ON K2K 0L1, Canada.

Testing was conducted in two phases,

- Initial testing took place from September 10 -19th, 2018.
- Formal testing for Common Criteria took place from November 19-22nd and November 30th, 2018.

The TOE was located in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. At the end of each day, the device was turned off. All evaluation documentation was kept with the evaluator at all times. The customer was involved in the execution of the test cases with the evaluators' guidance.

# 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 document: Detailed Test Report (DTR) and the Evaluation Technical Report (ETR).

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 Ciena Waveserver Ai Rel 1.3 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDcPP.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

## 9.1 Evaluation of Security Target

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 Ciena Waveserver Ai Rel 1.3 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP.

## 9.2 Evaluation of Development Documentation

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's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP related to the examination of the information contained in the TOE Summary Specification.

## 9.3 Evaluation of Guidance Documents

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 guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP related to the examination of the information contained in the operational guidance documents.

## 9.4 Evaluation of Life Cycle Support Activities

The evaluation team found that the TOE was identified.

The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes

hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing.

### 9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

### 9.6 Vulnerability Assessment Activity

The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

- http://nvd.nist.gov/

The evaluator selected the search key words based upon the following criteria.

- The vendor name was searched,
- The product name was searched,
- Key platform features the product leverages were searched

The vulnerability searches were performed on 19th October 2018, 20th March 2019 and 10th June 2019.

### 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 performed the Assurance Activities in the NDcPP, 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 evaluated configuration instructions in the *Ciena Waveserver Ai Rel 1.3 Common Criteria Guidance Document, v1.1, June 19, 2019* document. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

# 11 Annexes

Not applicable.

# 12 Security Target

Ciena Waveserver Ai Rel 1.3 Security Target v2.6, June 14, 2019.

# 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.
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 + Errata 20180314, Version 2.0e