National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Ciena 6500 Packet Optical Platform

Report Number: CCEVS-VR-VID10922-2018
Version 1.0
September 30, 2018

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 George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Patrick Mallett, PhD.
The MITRE Corporation

Jean Petty
The MITRE Corporation

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Ciena 6500 Packet Optical Platform provided by Ciena, Inc. 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 Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in September 2018. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the Network Device collaborative Protection Profile, version 2.0 + Errata 20180314 (NDcPP).

The Target of Evaluation (TOE) is the Ciena 6500 Packet Optical Platform, running the software release 12.3.

The Ciena 6500 S-Series and D-Series Packet Optical Platform is a family of standalone hardware devices that provide OSI Layer 0/1/2 network traffic management services. The 6500 series platforms enable users to direct traffic to designated ports, giving them control of network availability for specific services. However, the evaluated TOE functionality includes only the security functional behavior that is defined in the claimed NDcPP. The 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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the NDcPP. 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 is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the NDcPP Assurance Activities. 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 *Ciena 6500 Security Target v1.0*, dated August 6, 2018 and analysis performed by the Validation Team.

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 Compliant 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	Ciena 6500 Packet Optical Platform running the Ciena 6500 software release 12.3 Refer to Table 2 for Model Specifications
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	Ciena 6500 Security Target v1.0, dated August 6, 2018
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Ciena 6500" Evaluation Technical Report v1.0 dated September 5, 2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Ciena, Inc.
Developer	Ciena, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Patrick Mallett, PhD., The MITRE Corporation Jean Petty, The MITRE Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that the TOE is deployed in a physically secured operational environment and not subjected to any physical attacks.
- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- The TOE is not responsible for protecting network traffic that is transmitted across its interfaces that is not related to any TOE management functionality or generated data.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that regular software and firmware updates will be applied by a TOE Administrator when made available by the product vendor.
- Administrator credentials are assumed to be secured from unauthorized disclosure.
- TOE Administrators are trusted to ensure that there is no unauthorized access possible for sensitive residual information on the TOE when it is removed from its operational environment.

3.2 Threats

The following lists the threats addressed by the TOE.

- **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 includes 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.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional 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 level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.

- 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 security functionality 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 Security Target. The security monitoring of network traffic using IDS methods and statistical anomaly detection in order to safeguard networks against cyber-attacks functionality included in the product and described in Section 1.3 of the Security Target 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 of the TOE is the Ciena 6500 appliance described in Table 2 running the Ciena 6500 software release 12.3. In the evaluated configuration, the TOE uses SSH to secure remote command-line administration. and SSH to secure transmissions of security-relevant data from the TOE to external entities such as authentication server and syslog. The TOE includes administrative guidance in order to instruct Security Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

4 Architectural Information

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

4.1 TOE Introduction

The TOE is a network device as defined in the NDcPP which states: "This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device… A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network.". The TOE consists of the Ciena 6500 Packet Optical Platform, running the Ciena 6500 software release 12.3. Thus, the TOE is a network device composed of hardware and software.

4.2 Physical Boundary

The TOE is comprised of both software and hardware. The hardware is comprised of the following:

Model Type	Model Part #	SP2 Service Card PowerQUICC II Processor with VxWorks 6.3 NTK555CA NTK555EA NTK555FA	SPAP2 Service Card PowerQUICC II Processor with VxWorks 6.1 NTK555NA NTK555NB
2-slot Type 2	NTK503LA	No	Yes
7-slot	NTK503PA	Yes	No
7-slot Type 2	NTK503KA	No	Yes
6500-7	NTK503RA	Yes	No
14-slot	NTK503BA NTK503CA NTK503CC NTK503GA NTK503AD NTK503BD NTK503CD NTK503SA	Yes	No
32-slot	NTK603AA NTK603AB	Yes	No

Table 2 – Hardware Model Information

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

Component	Definition
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client, or locally, in which case

	the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications. Alternatively, the workstation can physically be connected to the TOE using the craft port, which is an Ethernet port through which the TOE can be managed locally using a SSH Client.
Audit Server	A general-purpose computer that runs a script to pull audit records from the TOE automatically, using the TL1 interface over SSH/secure file transfer protocol (SFTP).
Update Server	A server that supports SSH/SFTP and that is used as a location for storing product updates that can be transferred to the TOE.
Site Manager Software	The Site Manager software provides a graphical interface to the TL1 interface for managing the TOE. The Site Manager software is installed on the Management workstation and uses an SSH channel to connect to the TOE.

Table 5 – IT Environment Components

5 Security Policy

5.1.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE creates audit records for events related to security relevant events including authentication (success and failure, remote and local), cryptographic key management, session establishment (success and failure) and session termination, including for SSH communications. In addition, all actions corresponding to management functions are audited.
The TOE records, for each audited event, the date and time of the event, the type of event, the subject's claimed identity, and the outcome (success or failure) of that event. Depending on the specific type of event, additional data may be included in the audit record.
Audit data is stored locally and is pulled by a remote audit server via an automated script, using SFTP over an SSH trusted channel. The local audit data keeps the most recent records by overwriting the oldest records when the maximum size threshold of the file is met. No filesystem access is allowed to ensure protection of local audit data from deletion or modification.

5.1.2 Cryptographic Support

The TOE provides cryptography in support of SSH for remote administration, remote storage of audit data, and secure download of TOE updates. The TOE provides cryptography in support of SSH for remote administration, remote storage of audit data, and secure download of TOE updates. Diffie-Hellman group 14 asymmetric key generation and key establishment used by the TSF conforms to RFC 3526, Section 3. The TOE uses CAVP-validated cryptographic algorithms to ensure that appropriately strong cryptographic algorithms are used for these trusted communications:

SFR	Algorithm	CAVP Cert. #
FCS_COP.1/DataEncryption	AES	4855
FCS_RBG_EXT.1	DRBG	1706
FCS_COP.1/SigGen	ECDSA	1244
FCS_COP.1/KeyedHash	HMAC	3250
FCS_CKM.1 and FCS_COP.1/SigGen	RSA	2666
FCS_COP.1/Hash	SHS	3992

Table 5-1: Cryptographic Algorithm Certificates

Cryptographic keys are overwritten by zeroes by the TOE when they are no longer needed for their purpose.
The TOE collects entropy from a third-party hardware entropy source contained within the device to ensure sufficient randomness for secure key generation.

5.1.3 Identification and Authentication

All users must be identified and authenticated by the TOE before being allowed to perform any actions on the TOE, except viewing a banner. The TOE provides complexity rules that ensure that user-defined passwords will meet a minimum-security strength through the set of supported

characters and configurable minimum password length. As part of connecting to the TOE locally, using the management workstation, password data is obfuscated as it is inputted.
The TOE detects when a configurable number of failed authentication attempts are made by a remote user. Once this threshold of between 2 and 20 attempts has been met the TSF will automatically lock a user's account. The user's account can be unlocked after a configurable time period of between 0 and 7200 seconds or can be unlocked by a Security Administrator with sufficient UPC level (privilege).

5.1.4 Security Management

The TSF provides the TL1 interface for performing management functions remotely or locally. Also, the Security Administrator can use the Site Manager to pass commands to the TL1 interface. The functions that a Security Administrator can perform on the TL1 interface are determined by the Security Administrator's UPC value. The Security Administrator is the only administrative role that has the ability to manage the TSF, so it is the only role that is within the scope of the TOE. Apart from the Security Administrator, other roles that perform network management related functionality are not considered part of the TSF.

5.1.5 Protection of the TSF

The TOE is expected to ensure the security and integrity of all data that is stored locally and accessed remotely. The TSF prevents the unauthorized disclosure of secret cryptographic data, and administrative passwords are hashed using SHA-256. The TOE maintains system time with its local hardware clock. TOE software updates are acquired using SFTP and initiated using the TL1 interface. Software updates are digitally signed to ensure their integrity. The TSF also validates its correctness through the use of self-tests for both cryptographic functionality and integrity of the system software.

5.1.6 TOE Access

The TOE can terminate inactive sessions after a Security Administrator-configurable time period. The TOE also allows users to terminate their own interactive session. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session. The TOE can also display a configurable banner on the TL1 interface that is displayed prior to use of any other security-relevant functionality.

5.1.7 Trusted Path/Channels

The Security Administrator establishes a trusted path to the TOE for remote administration using SSH. An audit server establishes a trusted channel (SSH) to the TOE to pull audit data from the TOE using SFTP. The TOE establishes a trusted channel (SSH) for downloading software updates from the update server using SFTP.

Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- Ciena 6500 Supplemental Administrative Guidance for Common Criteria- v1.0
- Administration and Security Release 12.3, 323-1851-301
- TL1 Command Definition Release 12.3, 323-1851-190
- Site Manager for Ciena 6500 Packet-Optical Platform Fundamentals Release 12.3, 323-1851-195
- Supplemental Administrative Guidance for Common Criteria
- Suite of Hardware Installation Manuals: Release 12.3, 323-1851-201.(0-4)
    - General Information
    - 2, 7, 14, & 32 Slot Shelves (individual documents).

Any additional customer documentation 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 device as evaluated.

6 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Ciena 6500 Packet Optical Platform, running the software: Ciena 6500 version 12.3. Section 4.2 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to communicate with the following environment components:

- Management Workstation for local and remote administration. Workstation also has Site Manager Software installed.
- Audit Server for external storing of audit data that must support SSH/SFTP
- Update server for receiving software updates that must support SSH/SFTP

To use the product in the evaluated configuration, the product must be configured as specified in the *Ciena 6500 Packet Optical Platform Supplemental Administrative Guidance for Common Criteria Version 1.0* document.

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 *Assurance Activity Report for a Target of Evaluation "Ciena 6500 Packet Optical Platform" Assurance Activities Report v1.0 dated September 5, 2018.*

7.1 Test Configuration

The evaluation team configured the TOE for testing according to the *Ciena 6500 Packet Optical Platform Supplemental Administrative Guidance for Common Criteria Version 1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The evaluation team conducted testing at Ciena's facility in Hanover, MD on an isolated network within their facility. Testing was performed against the two management interfaces defined in the ST (local CLI and remote CLI).

The TOE was configured to communicate with the following environment components:

- Management Workstation for local and remote administration with Site Manager Software
- Audit Server for recording of audit data supporting SSH/SFTP
- Update server for receiving software updates supporting SSH/SFTP

The following test tools were installed on a separate workstation (management workstation)

- WireShark: version 2.6.2
- Bitvise SSH Client: version 7.31
- PuTTY .70

*Only the test tools utilized for functional testing have been listed.

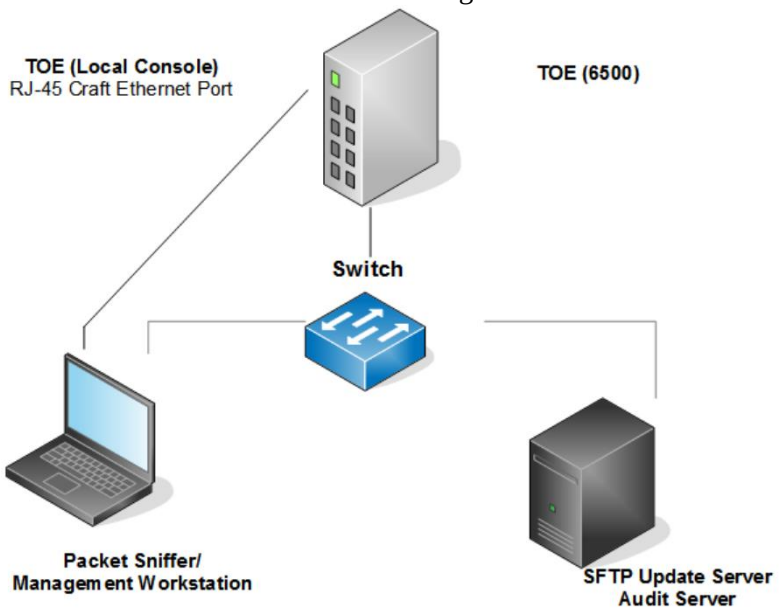

Figure 1 - Test Configuration

7.2 Developer Testing

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

7.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

7.4 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the NDcPP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	Description
Ciena	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
Packet Optical Platform	This is a generic term for searching for known vulnerabilities for the product family.
6500 Series	This is a generic term for searching for known vulnerabilities for the product family.
VxWorks 6.1 VxWorks 6.3	A specific version was not included in the search because this version may be within a range of vulnerable operating system versions and not listed separately.
SSH	This is a generic term for searching for known vulnerabilities for the SSH module on the 6500 series. A specific version was not included in the search because this version may be within a range of vulnerable versions and not listed separately.
TL1	Transaction Language 1 which is the command line interface environment for the TOE.

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources on August 20, 2018. The following public vulnerability sources were searched:

- NIST National Vulnerabilities: https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/
  https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search

- SecurITeam Exploit Search: www.securiteam.com
- Tenable Network Security http://nessus.org/plugins/index.php?view=search
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test enumerates network port and service information to determine if any ports were open and running services outside of the TOE standard configuration.
- CLI Privilege Escalation
  This attack involves enumerating a valid username with an attempt to access the underlying OS CLI shell, then cracking the user's password and logging in.
- Force SSHv1
  This attack determines if the client will accept both SSHv1 and SSHv2 connections when the TOE claims to only support SSHv2
- Fuzzing – Mutated TYPE and CODE
  This test determines if the TOE is adversely affected by the handling of large number of mutated IPv4, IPv6, ICMPv4, and ICMPv6 packets.
- Fuzzing – Mutated remaining field
  This test determines if the TOE is adversely affected by the handling of large number of mutated IPv4 and IPv6 packets where the header fields are carefully mutated to represent boundary cases, significant values, and randomly chosen values.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

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 ETR. The reader of this document can assume that all Evaluation 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 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

8.1 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 Ciena 6500 product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the NDcPP Supporting Documents in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validators 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 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's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents related to the examination of the information contained in the TOE Summary Specification.

The validators 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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

8.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Document related to the examination of the information contained in the operational guidance documents.

The validators 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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

8.4 Evaluation of the Life Cycle Support Activities (ALC)

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

The validators 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 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 NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validators reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

8.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validators 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 addressed the vulnerability analysis requirements in the NDcPP Supporting Documents, 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 performed the Evaluation Activities in the NDcPP Supporting Document, and correctly verified that the product meets the claims in the ST.

9 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Ciena 6500 Supplemental Administrative Guidance for Common Criteria Version 1.0* 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 audit server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

10 Annexes

Not applicable

11 Security Target

The security target for this product's evaluation is *Ciena 6500 Packet Optical Platform Security Target v1.0*, dated August 6, 2018.

12 List of Acronyms

Acronym	Definition
CC	Common Criteria
CLI	Command-Line Interface
cPP	collaborative Protection Profile
CRL	Certificate Revocation List
CVL	Component Validation List
DRBG	Deterministic Random Bit Generator
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NDcPP	Network Device collaborative Protection Profile
NIAP	National Information Assurance Partnership
OS	Operating System
OSI	Open Systems Interconnection
PP	Protection Profile
RBG	Random Bit Generator
SAR	Security Assurance Requirement
SCP	Secure Copy Protocol
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
ST	Security Target
TL1	Transaction Language One
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

13 Terminology

Term	Definition
TL1 [Management Interface]	The Transaction Language 1 (TL1) management interface is a TL1-compatible command shell interface that can be used to administer the TOE locally or remotely using SSH. This is used to perform functions that may be modified during ongoing administration of the TOE. The TL1 interface can be used by Site Manager or for direct CLI invocation.
Security Administrator	The Security Administrator is an authorized administrator of the TOE for particular management functions. The set of functions that a given user account is determined by the Administrator's User Privilege Code (UPC), which is a value in the range 1 to 5.
User Privilege Code	A User Privilege Code (UPC) is a numerical value that is associated with TOE functions and with administrative accounts. An administrative account is authorized to perform a given function if its UPC is greater than or equal to that of the desired function.
Authorized Administrator	The claimed Protection Profile defines an Authorized Administrator role that is authorized to manage the TOE and its data.
Entropy	A string of quasi-random data that is generated by unpredictable physical and/or logical phenomena in a computer and is used in the generation of random numbers.
Security Administrator	Synonymous with Authorized Administrator.
Trusted Channel	An encrypted connection between the TOE and a trusted remote server.
Trusted Path	An encrypted connection between a remote administrative interface and the TOE.

14 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018
6. Ciena 6500 Security Target v1.0, dated August 6, 2018
7. Ciena 6500 Release Supplemental Administrative Guidance for Common Criteria Version 1.0
8. GigaVUE-OS-CLIUsersGuide-v5100
9. GigaVUE-OS-HVUE-UsersGuide-v5100
10. GV-HC1-Series-HardwareInstallationGuide-v5100
11. GV-HC2- Series-HardwareInstallationGuide -v5100
12. GV-HC3-Series-HardwareInstallationGuide-v5100
13. GV-HD-Series-HardwareInstallationGuide-v5100
14. GV-TA-Series-HardwareInstallationGuide-v5100
15. Assurance Activity Report for a Target of Evaluation “Ciena 6500 Packet Optical Platform” Assurance Activities Report v1.0 dated September 5, 2018