National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1

Report Number: CCEVS-VR-VID10460-2012
Version 1.0
November 26, 2012

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

Table of Contents

1 EXECUTIVE SUMMARY 4
2 EVALUATION DETAILS 5
3 IDENTIFICATION 6
4 SECURITY POLICY 7
4.1 SECURITY AUDIT 7
4.2 CRYPTOGRAPHIC SUPPORT 7
4.3 USER DATA PROTECTION 7
4.4 IDENTIFICATION AND AUTHENTICATION 8
4.5 SECURITY MANAGEMENT 8
4.6 PROTECTION OF THE TSF 8
4.7 RESOURCE UTILIZATION 9
4.8 TOE ACCESS 9
4.9 TRUSTED PATH/CHANNELS 9
5 THREATS, OSPS, AND ASSUMPTIONS 10
5.1 THREATS TO SECURITY 10
5.2 ORGANIZATIONAL SECURITY POLICIES 10
5.3 PERSONNEL ASSUMPTIONS 10
5.4 PHYSICAL ASSUMPTIONS 10
6 CLARIFICATION OF SCOPE 12
6.1 SYSTEM REQUIREMENTS 12
6.2 CRYPTOGRAPHIC ASSURANCE 13
7 ARCHITECTURAL INFORMATION 14
7.1 TOE COMPONENTS 14
8 DOCUMENTATION AND DELIVERY 15
9 IT PRODUCT TESTING 16
9.1 FUNCTIONAL TESTING 16
9.1.1 Functional Test Methodology 16
9.1.2 Functional Results 16
9.2 VULNERABILITY TESTING 17
9.2.1 Vulnerability Test Methodology 17
9.2.2 Vulnerability Results 18
10 RESULTS OF THE EVALUATION 19
11 VALIDATOR COMMENTS/RECOMMENDATIONS 20
11.1 LACK OF NOTIFICATION OF AUDIT STORAGE EXHAUSTION 20
11.2 SECURE INSTALLATION AND CONFIGURATION DOCUMENTATION 20
12 SECURITY TARGET 21
13 LIST OF ACRONYMS 22
14 TERMINOLOGY 24
15 BIBLIOGRAPHY 25

1 Executive Summary

The Target of Evaluation (TOE) is the Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1. The TOE was evaluated by the Booz Allen Hamilton Common Criteria Test Laboratory (CCTL) in the United States and was completed in November 2012. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3. The evaluation was for Evaluation Assurance Level 2. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1 (herein referred to as the TOE) receives data from an external source and forwards that data to one or many ports. The TOE is part of the Carrier Ethernet technology. Carrier Ethernet provides a way to deliver Ethernet services across many networks while providing bandwidth management. The TOE operates on QoS capabilities and virtual switching functions to deliver different amounts of data to various ports. The TOE also contains next-generation Ethernet features that transport different Ethernet services through fiber or copper connections.

The various Ciena appliances which represent the TOE, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the TOE's Security Target.

The cryptography used in this product has not been FIPS-certified, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The technical information included in this report was largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the evaluation team. The ETR identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the product by any agency of the US Government and no warranty of the product is either expressed or implied.

2 Evaluation Details

Evaluated Product	Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1
Sponsor & Developer	Ciena Corporation, Linthicum, Maryland
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	November 2012
CC	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Evaluation Class	EAL2
Description	The TOE is a family of network device hardware appliances developed by Ciena Corporation. The validated models include the 3900 series, 5100 series, 5305, and 5410.
Disclaimer	The information contained in this Validation Report is not an endorsement of the TOE by any agency of the U.S. Government, and no warranty of the Security Management product is either expressed or implied.
PP	None
Evaluation Personnel	Justin Fisher John Schroeder Jeremy Sestok Amit Sharma
Validation Body	NIAP Common Criteria Evaluation and Validation Scheme

3 Identification

The product being evaluated is Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1

4 Security Policy

4.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. Each audit record contains the user information, time stamp, message briefly describing what actions were performed, outcome of the event, and severity. All audit record information is associated with the user of the TOE (if applicable). The TOE also maintains the ability to allow an authorized user to set and configure the settings for forwarding the data to the SNMP server. The TOE allows all users to view the log files. Only users of Admin-level or above can view the commands requiring Super User-level access. All audit data is displayed to users in a user-readable format. The TOE also contains mechanisms to notify the user upon detection of a potential security violation, including failed authentication, temperature threshold exceeded, fan failure, link status change, and line card failure. The TOE notifies external entities of detected faults through the usage of SNMP traps. Security violations are also recorded in the log files. Audit data generated to an external device can be configured to be sent to one or more syslog collectors. The transmission of audit data to syslog collectors is dependent on the syslog threshold configured on the TOE. The TOE does not allow any of the users to modify the audit logs. When the collector becomes full the TOE will overwrite the oldest log with the new audit information collected.

4.2 Cryptographic Support

SSHv2 is the protocol that allows connections to the TOE. SSH authentication generates a 256-bit AES key each time the user initiates with the TOE. The TOE also uses SSH to generate the public and private key pair. Only users with the Admin role can issue commands for key generation and deletion. SSH is used by the TOE for all user sessions through the CLI and is protected using standard SSH encryption practices. The SNMP traffic, as well as password information that is either sent or stored on the TOE, is encrypted throughout transit using SNMPv3 encryption standards.

4.3 User Data Protection

The TOE's core functionality is to receive data packet frames on its physical ports, traverse the data frames through its internal flow processing functionality, and forward the traffic to an associated destination port. The TOE allocates or de-allocates memory depending on the resources needed to complete the forward. The TOE also allows for authorized Admin or higher privileged users to define and map services to physical ports. In all systems where PBB-TE is used on incoming traffic, the TOE applies PBB-TE services to the ingress data frames to forward the traffic to the appropriate port. All traffic must pass through the virtual switch or VLAN in order for it to be forwarded. All VLAN traffic is forwarded based upon the tags contained within the header field. This varies between the type of VLAN traffic, of which PBB-TE is a type of traffic used. The TOE determines the order of egress traffic based on the QoS and CoS schemes.
The TOE enforces its information flow control policy based on different specifications on the system. The TOE maintains access control lists, MAC assignments, MAC learning tables, and management VLAN. These controls allow the TOE to explicitly allow and/or

deny information flow throughout the TOE. Additionally, customer premise equipment can be authenticated through the use of 802.1x.

4.4 Identification and Authentication

The TOE and its configured authentication services maintain distinct user accounts which contain the following attributes: user name, password, and role. The access rights correspond with the user's role on the system within a session object. If a user becomes logged out of the TOE either through the user logging his or herself out, or because of inactivity on the TOE, the changes will be reflected immediately and the user must re-enter credentials to log in to the TOE. All users must identify and authenticate before performing any TSF-mediated actions. The TOE supports authentication through its local database, as well as through the RADIUS and/or TACACS+ services. Multiple authentication methods can be configured in a hierarchical structure to prevent access failure by enabling the next authentication method in the list when the current method fails. TACACS+ associates the privilege level with each authenticated user on the TOE. When users are entering their passwords for authentication, the TOE does not display the clear text of the password to the user, but displays an obscured character feedback such as dots. Upon failed authentication attempts, the TOE will only display a message to the user stating that the user's logon was not permitted.

4.5 Security Management

The TOE maintains distinct roles for user accounts: Limited, Admin, and Super. These roles define the management functions for each user on the TOE. The Admin role is not available in SAOS version 6.9. For any references to functions requiring the Admin role, it can be assumed that these functions require the Super role in SAOS version 6.9. The Limited user is a read-only user, so any commands the user performs on the TOE will only allow the user to view different attributes and settings. The next level role is the Admin user who can perform all system configurations with the exception of managing users. Following the Admin role is the Super role. Super users can perform all system configurations including user management, including creating and deleting users on the TOE. Users with the minimum Admin-level privilege have the ability to configure the Ciena Carrier Ethernet Flow Control SFP.

The major functional areas of the TOE include managing flow control policy, users, and general configuration. These areas are restricted to those users with necessary minimum role or higher.

4.6 Protection of the TSF

The TOE maintains a secure state upon a port-link failure by allowing a transfer of primary service links. In the event of a Control Card failure in a chassis-based TOE, the TOE has the capability to remain in a secure state. The TOE performs POSTs to ensure the system is in a fully operational mode during start-up. The TOE checks the hardware upon start-up including CPU registers and memory space. If the TOE observes any fault or error, an alert will be published to the user. The TOE's internal system clock allows the user to see an accurate time of the failure. The system clock can be kept accurate through the use of time synchronizations with external NTP servers. Fault tolerance is also applied for the failure of any Control Card. If a Control Card fails, the secondary or backup Control Card will assume the TOE functionality. The TOE maintains the ability

to test its link quality and performance because the configuration file is verified on the backup Control Card. Users will not be able to verify any additional TOE information other than the status of the CPU registers and memory space information as well as the TOE configuration data.

4.7 Resource Utilization

The TOE maintains fault tolerance capabilities to maintain forwarding functionality in the occurrence of a Control Card failure in a chassis system or a service link failure in a connection with redundant physical connections. As an example, the Control Card provides a "heartbeat" to the monitoring standby card. If the "heartbeat" is lost, the standby card will then perform a switch-over to a 'mirror image' card.
The TOE uses PBB-TE or sub-ports to apply QoS schemes to the data frames sent over the system. With QoS, the TOE can provision and reserve appropriate bandwidth for each data stream to maintain a steady tunneling of traffic.

4.8 TOE Access

The TOE allows users to view a configurable banner upon establishing the user session. Only Limited users are not allowed to configure the banner for the TOE. The TOE is able to disconnect inactive users if the users' session reaches the configured inactivity time threshold. Each user can initiate the termination of the associated user session by entering the "exit" command. The TOE also has a maximum number of concurrent sessions for each user role as well as for SSH connections, and therefore can deny users access based on the number of sessions currently established.

4.9 Trusted Path/Channels

Connections to and from the TOE are protected using the protocols mentioned within the Cryptographic Support section. Trusted paths are used to secure all CLI sessions through SSH. Users initiate the trusted path to the TOE through establishing an SSH connection. The trusted path is used for authentication and all user management functions. All connections for the TOE are protected using the SSH cryptographic mechanism.

5 Threats, OSPs, and Assumptions

5.1 Threats to Security

Table 1 summarizes the threats that the evaluated product addresses.

Table 1 – Threats

T.ACCESS - A legitimate user of the TOE could gain unauthorized access to resources or information protected by the TOE, or perform operations for which no access rights have been granted, via user error, system error, or other actions.
T.ADMIN_ERROR - An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms.
T.AUDIT_COMPROMISE - A malicious user or process may view audit records, cause the records or information to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.DATA_COMPROMISE - A malicious user or process may attempt to gain unauthorized access and/or obtain resources controlled by the TOE that have been allocated during a TOE operational session.
T.EAVESDROPPING - A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.NETWORK_FLOW - A malicious user may attempt to subvert the TOE or defeat the operation of its security mechanisms to cause a disruption in the flow of data on the production network.
T.MASK - Users, whether they are malicious or non-malicious, could gain unauthorized access to the TOE by bypassing identification and authentication countermeasures.
T.STEALTH - A malicious user or process could perform suspicious activities against objects in the Operational Environment without an Operational Environment user becoming aware of this behavior because the TOE's forwarding policy did not forward the information to the necessary tool per its configuration.

5.2 Organizational Security Policies

Table 2 – Organizational Security Policies

P.ACCESS_BANNER - The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

5.3 Personnel Assumptions

Table 3 – Personnel Assumptions

A.ADMIN - One or more users authorized by the Operational Environment will be assigned to install, configure and manage the TOE and the security of the information it contains.
A.NOEVIL - Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation.
A.PASSWORD - Users select passwords according to the strong password policy that has been configured by an administrative user and will protect their own authentication data.

5.4 Physical Assumptions

Table 4 – Physical Assumptions

A.CPE - Service Delivery Switches will only be deployed to connect to Customer Premise Equipment.
A.LOCATE - The TOE will be located within controlled access facilities that will prevent unauthorized physical access.
A.PROTECT - The operational environment must protect the channel to the configured syslog collectors from interruption using logical methods, such as encryption, or physical methods such as disconnecting the TOE from internet and storing it in the same secure location.

6 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 (EAL 2 in this case).
- As with all EAL 2 evaluations, 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 TOE includes all the code that enforces the policies identified (see Section 4).

The evaluated configuration of the TOE includes the Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1 product that is comprised of one or more of the following:

- 3900 Series with SAOS 6.9.1.148
- 5100 Series with SAOS 6.9.1.148
- 5305 with SAOS 7.1.0.566
- 5410 with SAOS 7.1.0.566

6.1 System Requirements

The following components are present on the appliances for the TOE:

CES 5305

- RS-232 to Serial port (excluded)
- Ethernet Management port
- Data Hardware Interfaces port (fiber/copper)
- Alarm Interface (excluded)
- (2) Front-Loaded Redundant Dedicated Control Modules
- (5) Front-Loaded Hot-Swappable Line Modules
- (2) Front-Loaded Hot-Swappable Power Supplies
- (1) Front-Loaded Fan Tray

CES 3900 Series

- RS-232 to Serial port (excluded)

- Ethernet Management port
- Data Hardware Interfaces port (fiber/copper)
- (2) Redundant Power Supplies with integrated fans

CES 5100 Series

- RS-232 to Serial port (excluded)
- Ethernet Management port
- Data Hardware Interfaces port (fiber/copper)
- (1) DC Input Power Supply and/or (1) AC Input Power Supply
- (1) Field Replaceable Redundant Fan Tray

CES 5410

- RS-232 to Serial port (excluded)
- (2) DCN M Redundant Ethernet Management ports
- Data Hardware Interfaces port (fiber/copper)
- Alarm Interface (excluded)

In order to securely manage the TOE remotely, a management PC running SSH-capable terminal emulation software must be present in the Operational Environment.

6.2 Cryptographic Assurance

The cryptography used in this product has not been FIPS-certified, nor has it been analyzed or tested to conform to FIPS 140-2 cryptographic standards as part of this evaluation. The vendor has asserted that all cryptography used by the product has been tested.

7 Architectural Information

The TOE's boundary has been defined in Figure 1.

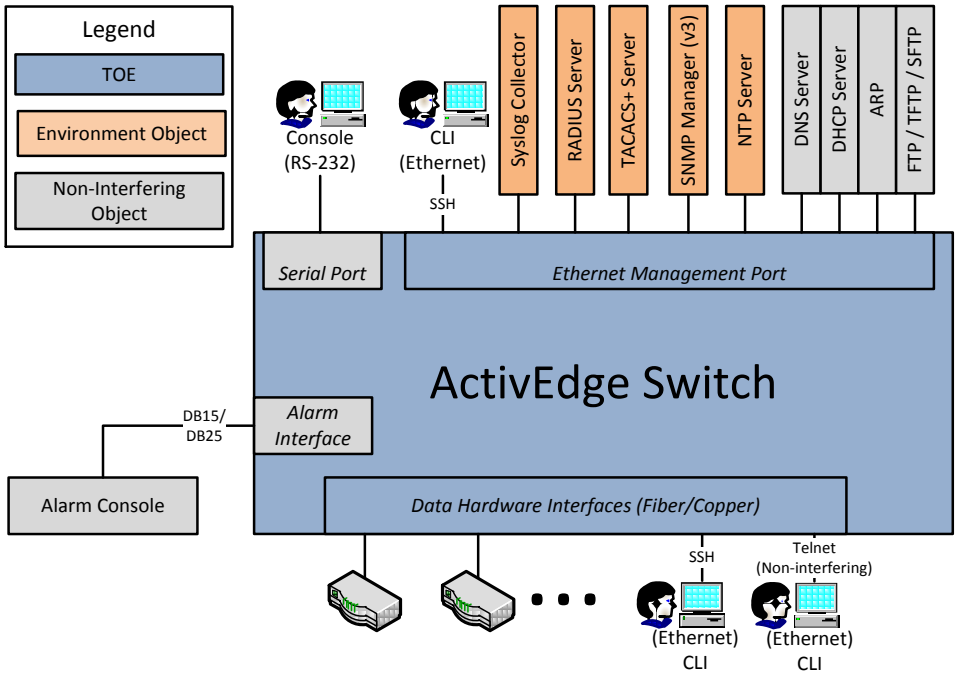

Figure 1 – TOE Boundary

7.1 TOE Components

The TOE is a hardware appliance and software based product. Thus, each CES model described in Section 6 is the TOE and the only component of the TOE.

8 Documentation and Delivery

The NIAP-certified Ciena CES product is acquired via normal sales channels.

The following documents were included within the scope of the evaluation:

- 5150 Service Aggregation Switch, Hardware Installation Manual
- 3930 Service Delivery Switch, Hardware Installation Manual
- 3960 Service Delivery Switch, Hardware Installation Manual
- 5305/LE-330 Service Aggregation Switch, Hardware Installation Manual
- 5410 Service Aggregation Switch, Installation and Startup
- SAOS Release Notes, Release 6.9.0.234
- SAOS Software Configuration Guide Release 6.9.0
- SAOS CLI Reference Manual, Release 6.9.0
- 5410 and 5306 Service Aggregation Switches, Release Notes, SAOS 7.1.0.498
- 5410 and 5306 Service Aggregation Switches, SAOS Software Configuration Guide 7.1.0
- 5410 and 5306 Service Aggregation Switches, SAOS CLI Command Reference 7.1.0
- Carrier Ethernet Solutions Service Delivery and Aggregation Switches, CCEVS Compliance Configuration, Releases 6.9 and 7.1, Revision A September 2012

IT Product Testing

8.1 Functional Testing

8.1.1 Functional Test Methodology

The test team's test approach is to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior either remotely, or on the platform. Each TOE external interface is described in the appropriate design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design (TDS), Functional Specification (FSP), and the vendor's test plans were used to demonstrate test coverage of all *appropriate* EAL2 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that were 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 executed a subset of the vendor functional testing. It has been determined that a sampling of the tests can be taken such that each SFR is tested to an appropriate level. The evaluation team also supplemented the vendor test cases with their own independent test plan to address any gaps in the coverage of SFRs.

The evaluators have determined that the vendor functional testing is a majority representation of the SFR and TSS claims made in the ST regarding the security functional requirements. However, the evaluators felt that additional testing was needed in order to verify the validity of the developer test environment and to provide additional assurance of the functionality of the TOE.

8.1.2 Functional Results

During the course of the evaluation, the Booz Allen evaluation team reviewed the vendor’s functional testing and determined that all *security relevant* TOE external interfaces were tested and a majority of the claimed functionality was tested by the vendor. The evaluation team then created a test plan that contained a sample of the vendor functional test suite, and supplemental functional testing developed by the evaluators. The evaluators test suite emphasized on the product’s primary functionality and any areas that required testing for claimed functionality. Based upon the results of the vendor and evaluator testing; it has been determined that the product functionally operates as described.

8.2 Vulnerability Testing

8.2.1 Vulnerability Test Methodology

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The Evaluation Team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

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:

- Eavesdropping on Communications

  This test attempts to intercept any TOE involved network traffic. The attack machine will execute an arp poisoning attack so that all network traffic between two nodes on a switched LAN will be tunneled through the attack machine before it reaches its destination. A sniffer will then be used to analyze the network traffic and attempt to view any confidential information that may be passing over the network.

- Port Scanning

  This test attempts to identify any way to subvert the security of the TOE by executing a side channel attack. A port scanner will be run against all TOE systems in an attempt to identify any open ports. Any port on a system that accepts external connections could potentially represent an attack vector. This test will identify any such ports and will attempt to enumerate them to determine their original purpose.

- Vulnerability Scanner (Nessus)

  This test uses the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE.

- Denial of Service – TCP Malformed Packet Flooding

  This attack attempts to exercise the stability of the IP stack and its components by sending a large amount of TCP packets and malformed TCP packets in an attempt to overload the application. If successful, the TOE will crash and not allow any connections until the TOE is rebooted.

- Management Network Denial of Service (DoS)

  This attack attempts to utilize proof of concept code to perform a denial of service attack against OpenSSH and the FTP functionality used in the TOE. A successful attack will deny service to FTP or other management functionality in the TOE.

- CLI Privilege Escalation

This test attempts to break out of the command shell and allow the attacker access to the Linux operating system on which the TOE is based. A successful attack will allow for the execution of unauthorized commands and for unintended system configuration changes.

- MAC Flooding

This attack attempts to flood the local network with random MAC addresses. A successful attack will cause the switch to fail open in repeating mode and allow for unauthorized disclosure of network traffic.

- VLAN Hopping

This attack attempts to have a system jump from one VLAN to another. A successful attack will cause the system to be placed on an unintended VLAN, allowing an attacker unauthorized access to a network.

- SSH Shredding

This attack attempts to identify implementation weaknesses in the SSH handshake using a module built into the Nexpose security scanner.

8.2.2 Vulnerability Results

During the vulnerability testing, there were several issues discovered that could affect the security posture of a deployed system. All of these findings were fixed by a vendor update to the product as a result of the testing effort and are therefore not present in the Common Criteria certified version of the product.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the TOE meets the security requirements contained in the Security Target.

The criteria against which the TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the TOE is EAL2. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in November 2012. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

10 Validator Comments/Recommendations

10.1 Lack of Notification of Audit Storage Exhaustion

During the evaluation, it was observed that no notification is provided for audit storage exhaustion. Audit logs are generated in a circular buffer, and when the allocated storage space has been exhausted, the oldest log file is overwritten with a new file. Administrators are advised to enable remote logging using syslog so that audit data is stored in a location where it has a higher assurance of availability.

10.2 Secure Installation and Configuration Documentation

The "Carrier Ethernet Solutions Service Delivery and Aggregation Switches, CCEVS Compliance Configuration, Releases 6.9 and 7.1" document defines the recommendations and secure usage directions for the TOE as derived from testing.

10.3 Dual Control Card Failover in Chassis-Based TOE

The 5305 and 5410 appliances each contain module control cards that provide redundancy in the event of the failure of a single card. The evaluators also tested the behavior of the TOE in the event of both cards failing. The 5410 appliance maintains data plane logic in the chassis itself rather than the control cards, so a disruption in control card failure will not affect its ability to enforce information flow control beyond the inability of an administrator to manage the information flow control functionality until a control card has been restored. On the other hand, the 5305 appliance does have some data plane logic on its control cards, so information flow control is only enforced until MACs are unlearned (approximately five minutes), after which point the appliance is unable to continue forwarding traffic until at least one control card is restored.

11 Security Target

The security target for this product's evaluation is Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1 Security Target, Version 1.6, 21 September 2012.

12 List of Acronyms

Acronym	Definition
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ARP	Address Resolution Protocol
CAM	Content Addressable Memory
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCM	Continuity Check Messages
CES	Carrier Ethernet Solutions
CFM	Control Frame Monitor
CLI	Command-line Interface
CIR	Committed Information Rate
CoS	Class of Service
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAL	Evaluation Assurance Level
ESM	Ethernet Services Manager
EUV	Egress Untagged VLAN
FTP	File Transfer Protocol
HAL	Hardware Abstraction Layer
IP	Internet Protocol
IP-ACL	IP - Access Control List
IPC	Inter-Process Communication
IT	Information Technology
MAC	Media Access Control
MD5	RSA Message Digest 5
MEP	Maintenance End Point
MIB	Management Information Base
MIP	Maintenance Intermediate Point
NAS	Network Access Server
NIAP	National Information Assurance Partnership
NMS	Network Management System
NTP	Network Time Protocol
OAM	Operations, Administration, and Maintenance
OS	Operating System
PBB	Provider Backbone Bridging
PBB-TE	Provider Backbone Bridging – Traffic Engineering
PDU	Protocol Description Unit
PIR	Peak Information Rate
PP	Protection Profile
PVID	Port VLAN ID
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RLAN	Resolved Local Area Network
SAOS	Service Aware Operating System
SAP	Service Access Point
SAR	Security Assurance Requirement
SAS	Service Aggregation Switch

SDS	Service Delivery Switch
SFP	Security Function Policy
SFTP	Secure File Transfer Protocol
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
TWAMP	Two-Way Active Measurement Protocol
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

13 Terminology

Terminology	Definition
Admin	Read/Write role with Limited privileges that can also perform execute commands
BVID	Backbone VLAN identifier; attribute in PBB-TE
C-tag	Customer VLAN tag; Used to create VLANs within the customer domain
Control Card	Hardware card within the TOE that performs the control plane functionality
Control Plane	Monitors the system and maintains the signal based configuration as well as the OAM control protocols
Data Plane	Allows for Data flow
Diag	Diagnostic role with no restrictions on privileges
ISID	Instance Service Identifier tag; used for the classification of traffic in PBB-TE
Forward	The TOE's ability to associate ingress traffic with egress ports and transfer traffic by using virtual switches and/or VLANs
Limited	Read-only role; able to execute commands that do not change the state or configuration of the TOE
Line Card	Hardware card within the TOE that performs the switching functionality
Management Control Card	Hardware card within the TOE that performs the management plane functionality
Management Plane	Allows for the management of the system through user configuration
Middleware	Provides communication between subsystems
Privilege Level	Vendor-specific terminology synonymous with role
S-tag	Service VLAN tag
Service	A logical association of network traffic based upon packet headers indicative of a specific type of traffic
Service Aggregation Switch	Provides the aggregation of data through a network via virtual switches; as a black box, the key differentiators are port density and port speeds for scalability
Service Delivery Switch	Provides the delivery of data through VLANs ; as a black box, the key differentiators are port density and port speeds for scalability
Severity	Synonymous with log-level within audit data; Determines the likelihood of an audit event to disrupt the TOE functionality or security
Super	Read/Write/Create role with Admin privileges; Has user management privileges in addition to general TOE management functions

14 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 3.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 3.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 3.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.
5. Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1, Version 1.6, September 21, 2012
6. Evaluation Technical Report for a Target of Evaluation "Ciena Carrier Ethernet Solutions Service Delivery and Aggregation Switches, Release 6.9 and 7.1" Evaluation Technical Report v3.1 dated November 12, 2012.