National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Gigamon GigaVUE

Report Number: CCEVS-VR-VID10902-2018
Version 1.0
October 1, 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

Jerome Myers, Senior Validator
Aerospace Corporation

Meredith Hennan, Lead Validator
Aerospace Corporation

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Christopher Rakaczky
Joshua Jones

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 Gigamon GigaVUE Visibility Appliances provided by Gigamon, 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 *collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314* (NDcPP).

The Target of Evaluation (TOE) is the Gigamon GigaVUE Visibility appliance, running the GigaVUE software version 5.1.01 (GigaVUE for short). The GigaVUE's primary functionality is to use the Gigamon Forwarding Policy to receive out-of-band copied network data from external sources (TAP or SPAN port) and forward that copied network data to one or many tool ports for packet capture or analyzing tools based on user selected criteria. GigaVUE can also copy the network traffic itself when sitting in-line with the network flow using passive, inline and bypass taps or any combination. GigaVUE features extensive filtering abilities enabling authorized users to forward precise customized data flows of copied data from many sources to a single tool, from a single source to many tools, or from many sources to many tools. 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 *Gigamon GigaVUE Security Target v1.0*, dated August 21, 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	Gigamon GigaVUE Visibility appliance, running the Gigamon GigaVUE software version 5.1.01 Refer to Table 2, 3, and 4 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	Gigamon GigaVUE Security Target v1.0, dated August 21, 2018
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Gigamon GigaVUE" Evaluation Technical Report v1.0 dated August 29, 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	Gigamon, Inc.
Developer	Gigamon, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Jerome Myers, Senior Validator - Aerospace Corporation Meredith Hennan, Lead Validator - Aerospace 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. All other functionality provided by these devices, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, the GigaVUE's network traffic capture, filter, and forwarding capabilities described in Section 1.3 of the Security Target were not assessed as part of

this evaluation. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

The evaluated configuration of the TOE is the Gigamon GigaVUE appliance described in Table 2 running the Gigamon GigaVUE-OS software version 5.1.01. In the evaluated configuration, the TOE uses TLS/HTTPS to secure remote web-based administration, SSH to secure remote command-line administration. and TLS, HTTPS 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 Gigamon GigaVUE model, running the Gigamon GigaVUE software version 5.1.01. 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:

Property	HD8	HD4
Model Number	GVS-HD8A1 (AC power) GVS-HD8A2 (DC power)	GVS-HD4A1 (AC power) GVS-HD4A2 (DC power)
Size	14RU	5RU
Total Slots	8	5
Power	AC or DC	AC or DC
Control Cards	2 (10/100/1000M Mgmt. port Serial Console per Controller card)	1 (10/100/1000M Mgmt. port Serial Console per Controller Card)
Port Blades	PRT-H00-X12G04 Port Blade, 12x10Gb and 4x1Gb PRT-H00-X12TS Port Blade, H Series, 12x10G Time Stamp PRT-H00-X04G44 Port Blade, 4x10Gb and 32x10Gb PRT-H00-Q02X32 Port Blade, H Series, 2x40Gb and 32x10Gb PRT-HD0-Q08 Port Blade, H Series, 8x40Gb PRT-HD0-C06X24 Port Blade, HD Series, 6x100G QSFP28 cages + 24x10G cages PRT-HD0-C02X08 Port Blade, HD Series, 2x100G CFP cages + 8x10G cages PRT-HD0-C02X08A Port Blade, HD Series, 2x100G CFP2 cages + 8x10G cages	
Power Supplies	4	2
Processor	NXP QorIQ P2041	NXP QorIQ P2041
Fixed Ports	None	None
Configurable Ports	Provided by Port Blades	Provided by Port Blades

Table 2 – HD Series Properties

Property	HC3	HC2	HC1

Model Number	GVS-HC301 (AC power) GVS-HC302 (DC power)	GVS-HC2A1 (AC power) GVS-HC2A2 (DC power)	GVS-HC101 (AC power) GVS-HC102 (DC power)
Size	3RU	2RU	1RU
TAP Modules	None	TAP-HC0-D25AC0 TAP module, SX/SR Internal TAP module 50/125, 12 TAPs TAP-HC0-D25BC0 TAP module, SX/SR Internal TAP module 62.5125, 12 TAPs TAP-HC0-D35CC0 TAP module, LX/LR Internal TAP module, 12 TAPs TAP-HC0-G100C0 TAP and Bypass Module, Copper, 12 TAP or BPS pairs	TAP-HC1-G10040 TAP and Bypass module, 10/100/1000M Copper, 4 TAPs or BPC pairs
Bypass Combo Modules	BPS-HC3-C25F26 Bypass Combo Module, GigaVUE-HC3, 2 100Gb SR4 BPS pairs, 16 10G cages	BPS-HC0-D25A4G Bypass Combo Module 4 SX/SR 50/125 BPS pairs, 16 10G cages BPS-HC0-D25B4G Bypass Combo Module 4 SX/SR 62.5/125 BPS pairs, 16 10G cages BPS-HC0-D35C4G Bypass Combo Module 4 LX/LR BPS pairs, 16 10G cages BPS-HC0-Q25A28 Bypass Combo Module 2 40G SR4 BPS pairs, 8 10G cages	BPS-HC1-D25A24 Bypass Combo Module, 2 SX/SR 50/125 BPS pairs, 4 10G cages
Smart Modules	SMT-HC3-C05 GigaSMART, GigaVUE-HC3, 5x100G QSFP28 cages (includes Slicing, Masking, Source Port, and GigaVUE Tunneling De-Encapsulation software)	SMT-HC0-R GigaSMART, GigaVUE-HC2 rear module (includes Slicing, Masking, Source Port, and GigaVUE Tunneling De-Encapsulation software) SMT-HC0-X16 GigaSMART, GigaVUE-HC2 front module, 16 10G cages (includes Slicing, Masking, Source Port, and GigaVUE Tunneling De-Encapsulation software)	None
Port Modules	PRT-HC3-C08Q08 Port Module, 8x100G QSFP28 cages, 8x40 QSFP+ cages PRT-HC3-X24 Port Module, GigaVUE-HC3,	PRT-HC0-X24 Port Module, 24x10G (QSFP) PRT-HC0-Q06 Port Module, 6x40G (QSFP+) PRT-HC0-C02 Port	None

	24x10G	Module, 2x100G (QSFP28)	
Processor	Intel Atom C2758	NXP QorIQ P2041	Intel Atom C2358
Fixed Ports	10/100/1000M Mgmt. port Serial Console	10/100/1000M Mgmt. port Serial Console	10/100/1000M Mgmt. port Serial Console 12 1G/10G Ports (QSFP) 4 10/100/1000M Ports
Configurable Ports	Provided by Port Modules	Provided by TAP modules, Bypass Combo modules, Port Modules	Provided by TAP modules, Bypass Combo modules

Table 3 – HC Series Properties

Property	TA10	**TA40**	TA100
Model Number	GigaVUE-TA10 Edge Traffic Aggregation Node GVS-TAX01 (AC power) GVS-TAX02 (DC power)	GigaVUE-TA40 Edge Traffic Aggregation Node GVS-TAQ01 (AC power) GVS-TAQ02 (DC power)	GigaVUE-TA100 Edge Traffic Aggregation Node GVS-TAC01 (AC power) GVS-TAC02 (DC power)
Size	1RU	1RU	1RU
Processor	NXP QorIQ P2020	NXP QorIQ P2020	Intel Atom C2338
Fixed Ports	10/100/1000M Mgmt. port Serial Console 48 1G/10G Ports (SFP+) 4 10G/40G QSFP Ports	10/100/1000M Mgmt. port Serial Console 32 10G/40G QSFP Ports	10/100/1000M Mgmt. port Serial Console 32 100GB QSFP28 ports
Configurable Ports	None	None	None

Table 4 – TA Series Properties

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

Component	Definition
Certification Authority	A server that acts as a trusted issuer of digital certificates and distributes a CRL that identifies revoked certificates.
LDAP Server	A system that is capable of receiving authentication requests using LDAP over TLS and validating these requests against identity and credential data that is defined in an LDAP directory.
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 to access the CLI or a web browser (Microsoft Internet Explorer 11 or higher and Google Chrome 36 or higher) to access the web GUI, 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.
Syslog Server	The Syslog Server connects to the TOE and allows the TOE to send Syslog messages to it for remote storage. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
Update Server	A general-purpose computer that includes a web server and is used to store software update packages that can be retrieved by the TOE using TLS/HTTPS. The Update Server can be a server maintained by Gigamon or it can be set up locally in the Operational Environment by an administrator if the TOE's deployment prevents it from being able to access Gigamon's web domain.

Table 5 – IT Environment Components

5 Security Policy

5.1.1 Security Audit

Audit records are generated for various types of management activities and events. The audit records include the date and time stamp of the event, the event type and subject identity. In the evaluated configuration, the TSF is configured to transmit audit data to a remote Syslog Server using SSHv2, but audit data is also stored locally to ensure availability of the data if communications with the Syslog Server are unavailable. Local audit records are stored in "message" files which are rotated to ensure a maximum limit of disk usage is enforced. Only users with the Admin privilege can access or delete the log files. Users with the Admin privilege are considered trusted users and are therefore not expected to delete or modify the audit records.

5.1.2 Cryptographic Support

The TOE uses sufficient security measures to protect its data in transmission by implementing cryptographic methods and trusted channels. The TOE uses SSH to secure the remote CLI and Syslog Server trusted channels. The TOE also uses TLS/HTTPS to secure the trusted channels for the secure web GUI, Update Server and LDAP server. SSH communications are established using Diffie-Hellman group 14 while TLS communications are established using the ECC scheme using NIST curve P-256.
Cryptographic keys are generated using the CTR_DRBG provided by this module. The TOE erases all plaintext secret and private keys that reside in both RAM and non-volatile storage with zeroes. In the evaluated configuration, the TOE operates in "Secure Cryptography Mode" which is used to restrict algorithms to meet the PP requirements.

The following table contains the CAVP algorithm certificates:

SFR	Algorithm	CAVP Cert. #
FCS_CKM.1 FCS_COP.1/SigGen	ECDSA	#1492
FCS_CKM.2	CVL	#1981
FCS_COP.1/DataEncryption	AES	#5541
FCS_COP.1/Hash	SHS	#4447
FCS_COP.1/KeyedHash	HMAC	#3692
FCS_RBG_EXT.1	DRBG	#2196

Table 6 – Cryptographic Algorithm Table

5.1.3 Identification and Authentication

All users must be identified and authenticated to the TOE before being allowed to perform any actions on the TOE. This is true of users accessing the TOE via the local console, or protected paths using the remote CLI via SSH or web GUI via TLS/HTTPS. Users authenticate to the TOE using one of the following methods:

- Username/password (defined on the TOE)
- LDAP authentication
- Username/public key (SSH only)

The TSF provides a configurable number of maximum consecutive authentication failures that are permitted by a user. Once this number has been met, the account is locked for a configurable time interval. Passwords that are maintained by the TSF can be composed of upper case, lower case,

numbers and special characters. The Security Administrator can define the password length between 8 and 30 characters. Password information is never revealed during the authentication process including during login failures. Before a user authenticates to the device, a configurable warning banner is displayed.
As part of establishing trusted remote communications, the TOE provides X.509 certificate functionality. In addition to verifying the validity of certificates, the TSF can check their revocation status using a certificate revocation list (CRL). The TSF can also generate a Certificate Signing Request in order to obtain a signed certificate to install for its own use as a TLS server.

5.1.4 Security Management

The TOE defines two roles: Admin and Monitor. Each of these roles has varying levels of fixed privilege to interact with the TSF. The Admin role is able to perform all security-relevant management functionality (such as user management, password policy configuration, application of software updates, and configuration of cryptographic settings). The Monitor role provides view-only access to ports and configurations. Therefore, the term "Admin", used throughout this document, is considered to be a Security Administrator of the TSF. Management functions can be performed using the local CLI, remote CLI, or web GUI. All software updates to the TOE are performed manually.

5.1.5 Protection of the TSF

The TOE stores usernames and passwords in a password file that cannot be viewed by any user on the TOE regardless of the user's role. The passwords are hashed using SHA-512. Public keys are stored in the configuration database which is integrity checked at boot time. Key data is stored in plaintext on the hard drive but cannot be accessed by any user. The TOE has an underlying hardware clock that is used for keeping time. The time can be manually set by the administrator. Power-on self-tests are executed automatically when the FIPS validated cryptographic module is loaded into memory. The FIPS cryptographic module verifies its own integrity using an HMAC-SHA1 digest computed at build time. All binaries (e.g. executables, libraries), are located on a read-only partition and cannot be modified. In addition, the TOE has a configuration database that is integrity checked at boot time.
The version of the TOE (both the currently executing version and the installed/updated version, if different) can be verified from any of the administrative interfaces provided by the TSF. The TOE is updated via the Gigamon Update Server or the local Update Server via an HTTPS protected connection. The updated image is verified via a digital signature.

5.1.6 TOE Access

The TOE can terminate inactive local console, remote CLI or web GUI sessions after a specified time period. The default setting is 15 minutes. Users can also terminate their own interactive sessions. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session. The TOE displays an administratively configured banner on the local console or remote CLI and the web GUI prior to allowing any administrative access to the TOE.

5.1.7 Trusted Path/Channels

The TOE connects and sends data to IT entities that reside in the Operational Environment via trusted channels. In the evaluated configuration, the TOE connects with a Syslog Server using SSH to encrypt the audit data that traverses the channel. The TOE also connects with an LDAP server using TLS and to an Update Server using TLS/HTTPS. The Update Server may either be one maintained by Gigamon, or a local server that is deployed in the TOE's Operational

Environment. When accessing the TOE remotely, administrators interface with the TSF using a trusted path. The remote CLI is protected via SSH and the web GUI is protected by TLS/HTTPS.

6 Documentation

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

- Gigamon GigaVUE Supplemental Administrative Guidance for Common Criteria- v1.0
- GigaVUE-OS-CLIUsersGuide-v5100
- GigaVUE-OS-HVUE-UsersGuide-v5100
- GV-HC1-Series-HardwareInstallationGuide-v5100
- GV-HC2- Series-HardwareInstallationGuide -v5100
- GV-HC3-Series-HardwareInstallationGuide-v5100
- GV-HD-Series-HardwareInstallationGuide-v5100
- GV-TA-Series-HardwareInstallationGuide-v5100

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.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Gigamon GigaVUE appliance, running the software: Gigamon GigaVUE version 5.1.01. 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:

- Certificate Authority/CRL Distribution Point
- LDAP Server for remote authentication
- Management Workstation for local and remote administration
- Syslog Server for recording of syslog data
- Update server for receiving software updates

To use the product in the evaluated configuration, the product must be configured as specified in the *Gigamon GigaVUE Supplemental Administrative Guidance for Common Criteria Version 1.0* document.

8 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 "Gigamon GigaVUE" Assurance Activities Report v1.0 dated August 30, 2018*.

8.1 Test Configuration

The evaluation team configured the TOE for testing according to the *Gigamon GigaVUE 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 in the Booz Allen CCTL facility on an isolated network. Testing was performed against all three management interfaces defined in the ST (local CLI, remote CLI, and web GUI).

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

- The platform used for the Update, LDAP, CRL Distribution, Certification Authority server (192.168.1.3) was Linux 3.16.0-4-amd64 #1 SMP Debian 3.16.51-3 (2017-12-13) x86_64 GNU/Linux.
    - HTTPS server used was Server version: Apache/2.4.10 (Debian) Server
    - Certificate Authority/CRL Distribution Point (OpenSSL 1.0.1t)
    - LDAP Server for remote authentication (OpenLDAP 2.4.40)
    - Update server for receiving software updates

- The platform used for the Syslog server (192.168.1.152) was Linux 4.9.0-4-amd64 #1 SMP Debian 4.9.65-3 (2017-12-03) x86_64 GNU/Linux.
    - Syslog Server for recording of syslog data (rsyslogd 8.24.0)

- Management Workstation for local and remote administration:
  The following test laptops were installed in the 192.168.1.0/24 range as separate workstations (management workstation):
    - HP zBook Laptop with Windows 7
        - WireShark: version 2.6.2
        - Firefox Quantum: version 61.0.2
        - Bitvise SSH Client: version 7.31
    - HP zBook Laptop with Windows 10
        - WireShark: version 2.6.2
        - Firefox Quantum: version 61.0.2
        - Bitvise SSH Client: version 7.31
    - Dell Precision M4800 Laptop dual boot setup with Windows 10 and Debian Linux 3.16.51-3
        - WireShark: version 2.6.2
        - Bitvise SSH Client: version 7.31
        - PuTTY .70
        - nmap: version 7.70
        - Nessus Professional: version 7.1.3 (#120) LINUX
        - Burp Suite Professional: version 1.7.36
        - Firefox Quantum: version 61.0.2
        - Metasploit stable release 4.14

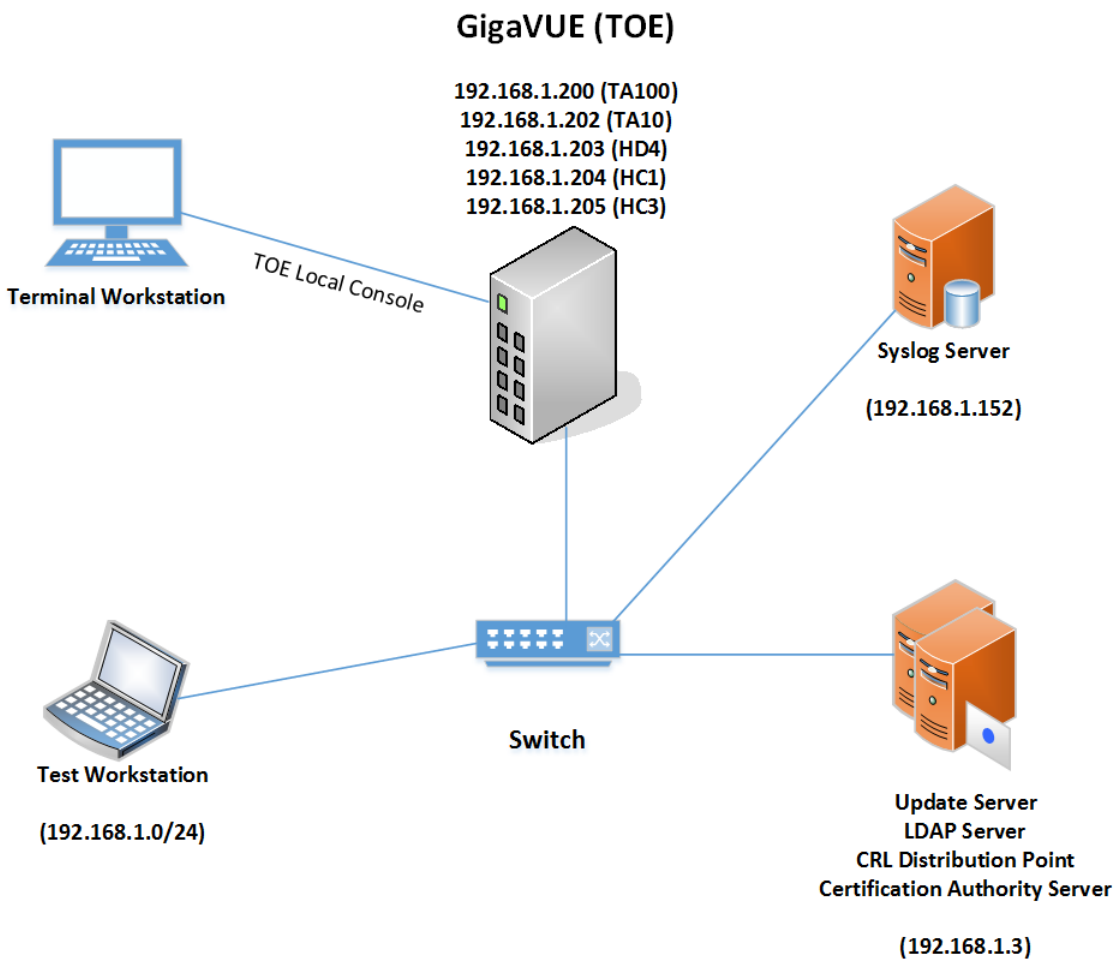

Figure 1 - Test Configuration

8.2 Developer Testing

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

8.3 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.

8.4 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
Gigamon	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
GigaVUE	This is a generic term for searching for known vulnerabilities for the specific product.
CentOS 5.8 **CentOS 6.6**	This is a generic term searching for known vulnerabilities for the underlying TOE operating system.
Gigamon Linux-Based Cryptographic Module	This is a generic term searching for known vulnerabilities for the TOE's cryptographic module.

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources on August 13, 2018, and updated October 1, 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 attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.

- Web Interface Vulnerability Identification (Nessus & Burp Suite)
  Burp Suite is a web application vulnerability assessment tool. It looks for major vulnerabilities including cross-site scripting, SQL injection, directory traversal, unchecked file uploads, etc. as well as less critical vulnerabilities such as unnecessary information disclosure. Nessus is a general-purpose network-based vulnerability scanner. It also looks for a suite of major vulnerabilities, including misconfigurations, default credentials, and web application related vulnerabilities.

- SSH Timing Attack (User Enumeration)
  This attack attempts to enumerate validate usernames for the SSH interface, by observing the difference in server response times to valid username login attempts.

- Force SSHv1
  This attack determines if the SSH server on the TOE will accept an SSHv1 connection when the TOE claims to only support SSHv2.

- Remote Network Scan (Nessus)
  Nessus is a general-purpose network-based vulnerability scanner. It also looks for a suite of major vulnerabilities, including misconfigurations, default credentials, and web application related vulnerabilities.

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

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all 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.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Gigamon GigaVUE 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.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target'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.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. 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.

9.4 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.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the 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.

9.6 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.

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 Evaluation Activities in the NDcPP Supporting Document, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Gigamon GigaVUE Supplemental Administrative Guidance for Common Criteria Version 1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that when the product is configured to offload audit files to an audit logging server, if that communications link is interrupted, the audit files generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit files generated during the outage. It will be necessary for the administrator to take steps to offload those files or they will be overwritten when the audit log is full.

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

The security target for this product's evaluation is *Gigamon GigaVUE Security Target v1.0*, dated August 21, 2018.

13 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
OSP	Organizational Security Policy
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
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

14 Terminology

Term	Definition
Administrator	A user who is assigned the Admin role on the TOE and has the ability to manage the TSF.
Security Administrator	The claimed Protection Profile defines a single Security Administrator role that is authorized to manage the TOE and its data. This TOE defines three separate user roles, but only the most privileged role (Admin) is authorized to manage the TOE's security functionality and is therefore considered to be the Security Administrator for the TOE.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application a Security Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to access the TOE functions or data.

15 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. Gigamon GigaVUE Security Target v1.0, dated August 21, 2018
7. Gigamon GigaVUE 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 “Gigamon GigaVUE” Assurance Activities Report v1.0 dated August 30, 2018