National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100

Report Number:	CCEVS-VR-11312-2022
Dated:	December 19, 2022
Version:	1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson
Sheldon Durrant
Lori Sarem
The MITRE Corporation

Farid Ahmed
Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Cornelius Haley
Katie Sykes
Douglas Kalmus
Ryan Hagedorn
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100 solution provided by Extreme Networks, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in December 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.

The TOE is the Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100 Security Target, Version 0.7, December 16, 2022 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100 (Specific models identified in Section 3.1)
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
ST	Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100 Security Target, Version 0.7, December 16, 2022
Evaluation Technical Report	Evaluation Technical Report for Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100, Version 0.3, December 16, 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Extreme Networks, Inc.
Developer	Extreme Networks, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Lori Sarem, and Farid Ahmed

3 Architectural Information

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

The TOE is the Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100. The TOE is a standalone network device that facilitates Data Link Layer data transfer between network nodes connected to its physical ports. TOE consists of a hardware appliance with embedded firmware. In the evaluated configuration, this consists of an instance of either of the VSP4900, VSP7400, VSP8400, or ExtremeAccess Platform (XA) models.

3.1 TOE Evaluated Configuration

The evaluated configuration consists of the VSP models shown in **Table 8-1** all running VOSS software version 8.3.100. The TOE links the Mocana 32-bit libraries with the Mocana GCM 64k feature enabled for cryptographic operations using non-PAA operations only.

Platform	Model	Processor
VSP 4900	VSP4900-48P	C3338 Intel Atom Denverton
	VSP4900-24S	C3338 Intel Atom Denverton
	VSP4900-24XE	C3538 Intel Atom Denverton
	VSP4900-12MXU-12XE	C3538 Intel Atom Denverton
VSP 7400	VSP7400 -32C	C3758 Intel Atom Denverton
	VSP7400-48Y-8C	C3758 Intel Atom Denverton
VSP 8400	VSP8404C	Freescale P2020 e500v2
ExtremeAccess Platform XA-1400	XA1440	C3558 Intel Atom Denverton
	XA1480	C3758 Intel Atom Denverton

Table 8-1 Extreme networking appliances - hardware

3.2 TOE Architecture

The basic architecture of each TOE appliance begins with a hardware appliance with physical network connections. Within the hardware appliance, the TOE is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing and switching functions).

There are normally two management interfaces – a browser-based management UI accessed via TLS/HTTPS and a CLI accessed locally or via SSH. However, to meet the requirements listed in the Security Target, the browser-based management UI must be disabled as described by guidance. Thus, in the evaluated configuration only the CLI can be used for management.

3.3 Physical Boundaries

The physical boundary of the TOE is the Extreme Networks Virtual Services Platform (VSP) Switches v8.3.100. These switches are running the VSP Operating System Software (VOSS) version 8.3.100, which includes:

- The appliance hardware
- RJ-45/RS-232 management ports

- USB port
- Embedded software/firmware installed on the appliance
- CLI management interface

Each TOE appliance runs a version of the Extreme proprietary OS and has physical network connections to its environment to facilitate routing and switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management. The TOE may be accessed and managed through a management workstation or terminal in the environment, which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to a syslog server in the environment. This is generally advisable given the limited audit log storage space on the evaluated appliances. The TOE sets its internal clock using administrative commands issued at the CLI interface or can use an NTP server.

The evaluation assumes the Operational Environment of the TOE includes the following:

- The SSH client that is used to access the management interface
- The management workstation that hosts the SSH client
- Syslog server for external storage of audit records
- NTP server for synchronizing system time
- Certificate Authority and OCSP servers to support X.509
- DNS server (optional)

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The Network Appliances provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: failure on invoking cryptographic functionality such as establishment, termination and failure of a TLS session; establishment, termination and failure of an SSH session; all use of the user identification mechanisms; any use of the authentication mechanism; any change in the configuration of the TOE, changes to time, initiation of TOE update, indication of completion of TSF self-test, termination of a remote session; and initiation and termination of a trusted channel.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using TLS. The logs for all appliances can be viewed from the CLI. The records include the date/time the event occurred, the event/type of event, the user ID associated with the event, and additional information of the event and its success and/or failure.

4.2 Cryptographic support

The TOE utilizes CAVP-tested cryptographic implementations to provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher-level cryptographic protocols. This cryptography is used to support the following features:

- TLS client in support of secure channel with remote syslog server,
- SSH server in support of secure CLI remote management interface,
- X.509 certificate validation and
- NTP support.

4.3 Identification and authentication

The TOE provides authentication services for administrative users to connect to the TOEs administrator interfaces (local CLI, and remote CLI). The TOE requires Administrators to authenticate prior to being granted access to any of the management functionality. In the Common Criteria evaluated configuration, the TOE requires a minimum password length be configured between 8 and 32 characters, as well as a minimum RSA key length of 2048 bits. The TOE provides administrator authentication against a local user database.

4.4 Security management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Management can take place over a variety of interfaces including:

- Local console command line administration;
- Remote command line administration via SSHv2;

The TOE provides multiple interfaces to perform administration. While in the CLI command mode, the administrator has access to six distinct modes, or privileges, that provide access to a specific set of commands. Depending on RBAC configuration, not every administrative account would have access to all modes. The CLI modes are as follows:

- User EXEC Mode: Initial mode of access.

- Privileged EXEC Mode: User mode and password combination determines access level.
- Global Configuration Mode: Use this mode to make changes to the running configuration.
- Interface Configuration Mode: Use this mode to modify or configure logical interface, VLAN or a physical interface.
- Router Configuration Mode: Use this mode to modify protocol settings.
- Application Configuration Mode: Use this mode to access the applications.

All administrative functionality is accessed via the CLI. The TOE audits all administrative access. The TOE displays login banners and inactivity timeouts to terminate idle administrative sessions after a set period of inactivity

4.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls restrictions to management and configuration functionality to Administrators. The TOE prevents reading of private keys and plaintext passwords by any user. The TOE internally maintains the date and time. This date and time are used as a timestamp that is part of each audit record generated by the TOE. Administrators can update the TOE's clock manually or can configure the TOE to synchronize with an external time source. The TOE performs testing to verify correct operation of the security appliances themselves. The TOE verifies all software updates via digital signature (2048-bit RSA/SHA-256) and requires administrative intervention prior to the software updates being installed on the TOE to avoid the installation of unauthorized firmware.

4.6 TOE access

The TOE can terminate inactive sessions after configurable period. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session. The TOE can also display specified banner on the local and remote CLI interfaces prior to allowing any administrative access to the TOE. The TOE allows users to manually terminate an established management session with the TOE.

4.7 Trusted path/channels

The TOE supports several types of secure communications:

- Trusted paths with remote administrators over SSH,
- Trusted channels with remote IT environment syslog servers over TLS.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020

That information has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

The evaluation was limited to the functionality and assurances covered in the NDcPP22e as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need 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 in accordance with the assurance activities specified in the NDcPP22e and performed by the Evaluation team.
- This evaluation covers only the specific device models and software as identified in this document (section 3.1), and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. In particular, the following features are not included in the scope of the evaluation:
    - Browser-based management UI accessed via TLS/HTTPS is disabled and is not evaluated.
    - The use of SNMPv3 is excluded.
    - Fabric Extend with IPsec is not evaluated.
    - Use of the FTP server is excluded and it is disabled by default.

- Integration with AAA server is not evaluated.
- Virtualized VOSS versions are not included in the scope and are not evaluated.

7 Documentation

The following documents were available with the TOE for evaluation:

- Extreme VOSS Common Criteria Configuration Guide 8.3.100, December 2022

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 Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100, Version 0.3, December 16, 2022 (AAR).

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to the Common Criteria Certification document and ran the tests specified in the NDcPP22e including the tests associated with optional requirements. Section 3.4.1 of the AAR lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8.3 TOE Testing Timeframe and Location

- Testing was conducted during the timeframe of November 2021 to November 2022.
- Testing was conducted at Gossamer Security Solutions CCTL located at Columbia, MD.

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 assurance 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 5 and CEM version 3.1 rev 5. The evaluation determined the Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

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 Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

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 ST and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP22e related to the examination of the information contained in the TSS.

The Validation reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

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 NDcPP22e and recorded the results in a Test Report, summarized in the AAR.

The Validation reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities and fuzz testing. None of the public search for vulnerabilities, or the fuzz testing uncovered any residual vulnerability.

The Evaluation team performed a public search for vulnerabilities in order to ensure there are no publicly known and exploitable vulnerabilities in the TOE from the following sources:

National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
Exploit / Vulnerability Search Engine (http://www.exploitsearch.net)
SecurITeam Exploit Search (http://www.securiteam.com)
Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
Offensive Security Exploit Database (https://www.exploit-db.com/)

The search was performed on December 15, 2022. The search was conducted with the following search terms: "Extreme", "VOSS", "VSP", "SSH", "TLS", "Intel Atom", "Freescale P2020”.

The Validation team reviewed the work of the Evaluation team, and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

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 testing also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 7 of this Validation Report. No versions of the TOE and software, either earlier or later were evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, should be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100 Security Target, Version 0.7, December 16, 2022.*

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020.

[5] Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100 Security Target, Version 0.7, December 16, 2022 (ST).

[6] Assurance Activity Report for Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100, Version 0.3, December 16, 2022 (AAR).

[7] Detailed Test Report for Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100, Version 0.3, December 16, 2022 (DTR).

[8] Evaluation Technical Report for Extreme Networks Virtual Services Platform (VSP) Series Switches v8.3.100, Version 0.3, December 16, 2022 (ETR)