National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Extreme Networks ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100

Report Number:	**CCEVS-VR-11301-2022**
Dated:	**October 28, 2022**
Version:	**0.2**

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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Anne Gugel
Lauren Hardy
Randy Heimann
Linda Morrison
Clare Parran
Chris Thorpe

Common Criteria Testing Laboratory

Cornelius Haley
Katie Sykes
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 3
3.1 TOE Evaluated Configuration 3
3.2 TOE Architecture 3
3.3 Physical Boundaries 3
4 Security Policy 7
4.1 Security audit 7
4.2 Cryptographic support 7
4.3 Identification and authentication 7
4.4 Security management 8
4.5 Protection of the TSF 8
4.6 TOE access 8
4.7 Trusted path/channels 8
5 Assumptions & Clarification of Scope 10
6 Documentation 11
7 IT Product Testing 12
7.1 Developer Testing 12
7.2 Evaluation Team Independent Testing 12
8 Evaluated Configuration 13
9 Results of the Evaluation 16
9.1 Evaluation of the Security Target (ASE) 16
9.2 Evaluation of the Development (ADV) 16
9.3 Evaluation of the Guidance Documents (AGD) 16
9.4 Evaluation of the Life Cycle Support Activities (ALC) 17
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 17
9.6 Vulnerability Assessment Activity (VAN) 17
9.7 Summary of Evaluation Results 18
10 Validator Comments/Recommendations 19
11 Annexes 20
12 Security Target 21
13 Glossary 22
14 Bibliography 23

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Extreme Networks ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100. 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 Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in October 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 Target of Evaluation (TOE) is the Extreme Networks ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100.

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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Extreme Networks ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100 Security Target Version 1.0, 10/25/2022 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 Product Compliant List (PCL).

Table 1 provides information needed to completely identify the product and its evaluation

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	Extreme Networks ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
ST	Extreme Networks ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100 Security Target, Version 1.0, 10/25/2022
Evaluation Technical Report	Evaluation Technical Report for Extreme Networks ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100 version 0.2, 10/25/2022
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 & Developer:	Extreme Networks, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	Anne Gugel, Lauren Hardy, Randy Heimann, Linda Morrison, Clare Parran, Chris Thorpe

3 Architectural Information

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

The Target of Evaluation (TOE) is the Extreme Networks ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100. The TOE provides high density layer 2/3 switching with low latency cut-through switching and IPv4 and IPv6 unicast and multicast routing to enable enterprise aggregation and core backbone deployments. The TOE consists of a hardware appliance with embedded software components.

3.1 TOE Evaluated Configuration

Details regarding the evaluated configuration is provided in Section 8 below.

3.2 TOE Architecture

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, and processor and software that implements routing and switching functions, configuration information and drivers. While hardware varies between different appliance models, the EXOS software is shared across all platforms.

EXOS is composed of subsystems designed to implement operational, security, management, and networking functions. Hardware-specific device drivers that reside in the kernel provide abstraction of the hardware components. A dedicated cryptographic module is integrated with protocol libraries that implement secure channel functionality. A control plane subsystem that includes Internet Protocol (IP) host stack, which can be further subdivided into protocol and control layers, implements switching and routing functions. A system management subsystem, that includes an Authentication, Authorization and Accounting (AAA) module, implements an administrative interface and maintains configuration information.

3.3 Physical Boundaries

The physical boundary of the TOE is the Extreme Networks ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100. EXOS is based on Linux Kernel version 4.14.200.

Model	CPU	CPU Mfg	CPU Type	Micro Architecture	CPU Cores
X440-G2-12t-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1

Model	CPU	CPU Mfg	CPU Type	Micro Architecture	CPU Cores
X440-G2-12p-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24t-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24p-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-48t-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-48p-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24t-10GE4-DC	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-48t-10GE4-DC	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24x-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24fx-GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-12t8fx-GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24t-GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X460-G2-24t-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-48t-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2

Model	CPU	CPU Mfg	CPU Type	Micro Architecture	CPU Cores
X460-G2-24p-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-48p-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-24x-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-48x-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-24t-GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-48t-GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-24p-GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-48p-GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-16mp-32p-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-24p-24hp-10GE4	CN6120	Marvell (formerly Cavium)Marvell	MIPS	Octeon II	2
X460-G2-24ht-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X435-8T-4S	Broadcom BCM53549	ARM	Cortex-A	Cortex-A72 Armv7	4
X435-8P-4S	Broadcom BCM53549	ARM	Cortex-A	Cortex-A72 Armv7	4
X435-8P-2T-W	Broadcom BCM53548	ARM	Cortex-A	Cortex-A72 Armv7	4
X435-24T-4S	Broadcom BCM53547	ARM	Cortex-A	Cortex-A72 Armv7	4

Model	CPU	CPU Mfg	CPU Type	Micro Architecture	CPU Cores
X435-24P-4S	Broadcom BCM53547	ARM	Cortex-A	Cortex-A72 Armv7	4
X465-24W	C3338	Intel	Atom	Denverton	2
X465-48T	C3338	Intel	Atom	Denverton	2
X465-48P	C3338	Intel	Atom	Denverton	2
X465-48W	C3338	Intel	Atom	Denverton	2
X465i-48W	C3538	Intel	Atom	Denverton	4
X465-24MU	C3538	Intel	Atom	Denverton	4
X465-24MU-24W	C3538	Intel	Atom	Denverton	4
X465-24S	C3338	Intel	Atom	Denverton	2
X465-24XE	C3538	Intel	Atom	Denverton	4
X695-48Y-8C	C3758	Intel	Atom	Denverton	8
5520-24T	Broadcom BCM56377	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-24W	Broadcom BCM56377	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-48T	Broadcom BCM56376	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-48W	Broadcom BCM56376	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-12MW-36W	Broadcom BCM56375	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-48SE	Broadcom BCM56376	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-24X	Broadcom BCM56375	ARM	Cortex-A	Cortex A72 ARMv8	4

The Operational Environment of the TOE includes:

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

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 TOE generates audit records for all security-relevant events. For each audited events, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event. The resulting records are stored locally and can be sent securely to a designated audit server for archiving. Security Administrators, using the appropriate CLI commands, can also view audit records locally. The TOE provides a reliable timestamp relying on the appliance's built-in clock or using an NTP server.

4.2 Cryptographic support

The TOE performs the following cryptographic functionality:

- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification utilizing a dedicated cryptographic library
- Cryptographic functionality is utilized to implement secure channels
  - SSHv2
  - TLS v1.2
- Entropy is collected and used to support seeding with full entropy
- Critical Security Parameters (CSPs) internally stored and cleared when no longer in use
- X509 Certificate authentication integrated with TLS protocol.

The TOE uses a dedicated cryptographic module to manage CSPs and implements deletion procedures to mitigate the possibility of disclosure or modification of CSPs. Additionally, the TOE provides commands to on-demand clear CSPs (e.g. host RSA keys), that can be invoked by a Security Administrator with appropriate permissions.

4.3 Identification and authentication

The TOE supports Role-Based Access Control (RBAC) managed by an Authentication, Authorization, and Accounting (AAA) module that stores and manages permissions of all users and their roles. The TOE requires users to provide their assigned unique username and password before any administrative access to the system is granted. Each authorized user is associated with an assigned role and role-specific permissions that determine their access to TOE features. The AAA module stores the assigned role of each user along with all other information required for that user to access the TOE.

The TOE supports X509v3 certificate validation during negotiation of TLS protected syslog. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE.

4.4 Security management

The TOE allows remote administration using an SSHv2 session, and local administration using a console. Both remote and local administration are conducted over a Command Line Interface (CLI) terminal that facilitates access to all of the management functions used to administer the TOE.

There are two types of administrative users within the system: Security Administrator and User. All of the management functions are restricted to Security Administrators, including: managing user accounts and roles, rebooting and applying software updates, administering the system configuration, and reviewing audit records. The term "Security Administrator" is used to refer to any administrative user with the appropriate role to perform the relevant functions

4.5 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features.

- The TOE protects CSPs, including stored passwords and cryptographic keys, so they are not directly viewable or accessible in plaintext.
- The TOE ensures that reliable time information is available for both log accountability and synchronization with the operating environment.
- The TOE performs self-tests to detect internal failures and protect itself from malicious updates.

4.6 TOE access

The TOE will display a customizable banner when an administrator initiates an interactive local or remote session. The TOE also enforces an administrator-defined inactivity timeout after which any inactive session is automatically terminated. Once a session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

4.7 Trusted path/channels

The TOE protects remote sessions by establishing a trusted path secured using SSH between itself and the administrator. The TOE prevents disclosure or modification of audit records by establishing a trusted channel using TLS between itself and the audit server. Mutual authentication using client-side x.509v3 certificates is supported by the TOE’s TLS client for syslog over TLS.

5 Assumptions & Clarification of Scope

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 scope of this 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.

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 with a certain level of assurance (the assurance activities specified in the Protection Profile for Network Devices and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, 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.

6 Documentation

The following documents were available with the TOE for evaluation:

- Extreme Networks ExtremeXOS Common Criteria Configuration Guide 31.3.100, Version 9037401-00, Rev AA, October 2022

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. Consumers are encouraged to download the CC configuration guide (CCECG above) from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report for Extreme Networks ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100, Version 1.0, October 25,2022 (AAR).

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according a 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 Evaluated Configuration

The evaluated configuration consists of the following series of appliances all running EXOS software version 31.3.100:

- ExtremeSwitching Series x440-G2
- ExtremeSwitching Series x460-G2
- ExtremeSwitching Series x435
- ExtremeSwitching Series x465
- ExtremeSwitching Series x695
- 5520 Series

Model	CPU	CPU Mfg	CPU Type	Micro Architecture	CPU Cores
X440-G2-12t-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-12p-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24t-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24p-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-48t-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-48p-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24t-10GE4-DC	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-48t-10GE4-DC	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24x-10GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24fx-GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1

Model	CPU	CPU Mfg	CPU Type	Micro Architecture	CPU Cores
X440-G2-12t8fx-GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X440-G2-24t-GE4	CN7010	Marvell (formerly Cavium)	MIPS	Octeon III	1
X460-G2-24t-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-48t-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-24p-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-48p-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-24x-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-48x-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-24t-GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-48t-GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-24p-GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-48p-GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X460-G2-16mp-32p-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2

Model	CPU	CPU Mfg	CPU Type	Micro Architecture	CPU Cores
X460-G2-24p-24hp-10GE4	CN6120	Marvell (formerly Cavium)Marvell	MIPS	Octeon II	2
X460-G2-24ht-10GE4	CN6120	Marvell (formerly Cavium)	MIPS	Octeon II	2
X435-8T-4S	Broadcom BCM53549	ARM	Cortex-A	Cortex-A72 Armv7	4
X435-8P-4S	Broadcom BCM53549	ARM	Cortex-A	Cortex-A72 Armv7	4
X435-8P-2T-W	Broadcom BCM53548	ARM	Cortex-A	Cortex-A72 Armv7	4
X435-24T-4S	Broadcom BCM53547	ARM	Cortex-A	Cortex-A72 Armv7	4
X435-24P-4S	Broadcom BCM53547	ARM	Cortex-A	Cortex-A72 Armv7	4
X465-24W	C3338	Intel	Atom	Denverton	2
X465-48T	C3338	Intel	Atom	Denverton	2
X465-48P	C3338	Intel	Atom	Denverton	2
X465-48W	C3338	Intel	Atom	Denverton	2
X465i-48W	C3538	Intel	Atom	Denverton	4
X465-24MU	C3538	Intel	Atom	Denverton	4
X465-24MU-24W	C3538	Intel	Atom	Denverton	4
X465-24S	C3338	Intel	Atom	Denverton	2
X465-24XE	C3538	Intel	Atom	Denverton	4
X695-48Y-8C	C3758	Intel	Atom	Denverton	8
5520-24T	Broadcom BCM56377	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-24W	Broadcom BCM56377	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-48T	Broadcom BCM56376	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-48W	Broadcom BCM56376	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-12MW-36W	Broadcom BCM56375	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-48SE	Broadcom BCM56376	ARM	Cortex-A	Cortex A72 ARMv8	4
5520-24X	Broadcom BCM56375	ARM	Cortex-A	Cortex A72 ARMv8	4

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 ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100 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 ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 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 validator 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 validator 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 identified.

The validator 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 validator 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>)
- 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 10/06/2022 with the following search terms: "Extreme", "EXOS", "XOS", "TLS", "SSH", "Intel Atom", "Cavium Octeon", "BCM53549", "OpenSSL

2.0.16", "BCM56375", "BCM56376", "BCM56377", "BCM53547", "BCM53548", "Broadcom".

The validator 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 Extreme Networks ExtremeXOS Common Criteria Configuration Guide 31.3.100, Version 9037401-00, Rev AA, October 2022. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, 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 is identified as: *ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100 Security Target version 1.0, October 25, 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] ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100 Security Target Version 1.0, 10/25/2022 (ST).

[6] Assurance Activity Report for ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100, Version 1.0, 10/25/2022 (AAR).

[7] Detailed Test Report for ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100, Version 1.0, 10/25/2022 (DTR).

[8] Evaluation Technical Report for ExtremeSwitching Series (x440-G2, x460-G2, x465, x435, x695) and 5520 Series Switches running EXOS 31.3.100, Version 0.2, 10/25/2022 (ETR)