

National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



Validation Report

Extreme Networks, Inc.

**NetIron Family Devices with Multi-Service IronWare
R06.3.00aa**

Report Number: CCEVS-VR-VID10998-2019
Dated: September 24, 2019
Version: 0.1

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

Paul Bicknell
Jenn Dotson
Randy Heimann
Clare Olin
Chris Thorpe
The MITRE Corporation
Bedford, MA

Common Criteria Testing Laboratory

Cornelius Haley
Wasif Sikder
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1	Executive Summary.....	1
2	Identification.....	1
3	Architectural Information.....	2
3.1	TOE Description.....	3
3.2	TOE Evaluated Configuration.....	3
3.3	Physical Scope of the TOE.....	3
4	Security Policy.....	4
4.1	Cryptographic support.....	4
4.2	Identification and authentication.....	4
4.3	Security management.....	4
4.4	Protection of the TSF.....	4
4.5	TOE Access.....	5
4.6	Trusted channels.....	5
5	Assumptions.....	5
6	Clarification of Scope.....	5
7	Documentation.....	6
8	IT Product Testing.....	6
8.1	Developer Testing.....	6
8.2	Evaluation Team Independent Testing.....	6
9	Evaluated Configuration.....	6
10	Results of the Evaluation.....	7
10.1	Evaluation of the Security Target (ASE).....	7
10.2	Evaluation of the Development (ADV).....	7
10.3	Evaluation of the Guidance Documents (AGD).....	7
10.4	Evaluation of the Life Cycle Support Activities (ALC).....	8
10.5	Evaluation of the Test Documentation and the Test Activity (ATE).....	8
10.6	Vulnerability Assessment Activity (VAN).....	8
10.7	Summary of Evaluation Results.....	9
11	Validator Comments/Recommendations.....	9
12	Annexes.....	9
13	Security Target.....	9
14	Glossary.....	9
15	Bibliography.....	10

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa. 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 August 2019. 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 2.1, 24 September 2018 (NDcPP21).

The Target of Evaluation (TOE) is the NetIron Family Devices with Multi-Service IronWare R06.3.00aa.

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, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa Security Target, Version 0.4, September 9, 2019 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.

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	Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018
ST	Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa (NDcPP21) Security Target, Version 0.4, September 9, 2019
Evaluation Technical Report	Evaluation Technical Report for Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa, version 0.3, September 24, 2019
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.
CCEVS Validators	

3 Architectural Information

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

The Target of Evaluation (TOE) is Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa.

The TOE is composed of a hardware appliance with embedded software installed on a management processor. The embedded software is a version of Extreme's proprietary Multi-Service IronWare software. The software controls the switching and routing network frames and packets among the connections available on the hardware appliances.

3.1 TOE Description

The basic architecture of each TOE appliance begins with a hardware appliance with physical network connections. Within the hardware appliance, the Extreme IronWare OS is designed to control and enable access to the available hardware functions (e.g., program execution, device access, facilitate basic routing functions). IronWare OS enforces applicable security policies on network information flowing through the hardware appliance.

During normal operation, IP packets are sent to the management IP address or through the appliance over one or more of its physical network interfaces, which processes them according to the system's configuration and state information dynamically maintained by the appliance. This processing typically results in the frames or packets being forwarded out of the device over another interface. The TOE will process other packets destined for itself (control path packets) based on the requirements of the given protocol (i.e., SSH).

3.2 TOE Evaluated Configuration

The Target of Evaluation (TOE) is Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa including the following series and models:

- Extreme NetIron MLXe Series Hardware Platforms
 - BR-MLXE-4-AC, BR-MLXE-8-AC, BR-MLXE-16-AC with management card BR-MLX-MR2-X
 - BR-MLXE-32-AC with management card BR-MLX-MR2-32-X
- Extreme NetIron CER 2000 Series Hardware Platforms
 - BR-CER-2024C-4X-RT
 - BR-CER-2024F-4X-RT.

While there are different models in the TOE, they differ primarily in physical form factor, number and types of connections and slots, and relative performance. There are some functional differences among the families, but they each provide the same security characteristics as claimed in this security target.

3.3 Physical Scope of the TOE

Each TOE appliance runs a version of the Extreme's software 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 PC 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 an external syslog server in the network environment. This is generally advisable given the limited audit log storage space on the evaluated appliances.

NetIron utilizes TLS protected TACACS+ and RADIUS authentication.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Cryptographic Support
2. Identification and Authentication
3. Security Management
4. Protection of the TSF
5. TOE Access
6. Trusted Channels

4.1 Cryptographic support

The TOE has CAVP-tested algorithms that provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including SSH and TLS.

4.2 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of passing network traffic in accordance with its configured switching/routing rules. It provides the ability to both assign attributes (user names, passwords and privilege levels) and to authenticate users against these attributes. The TOE utilizes x509.3 certificates to authenticate TLS services providing service to the TOE, and performs certificate status verification using OCSP protocol.

4.3 Security management

The TOE provides Command Line Interface (CLI) commands to access the wide range of security management functions to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users. Among the available privileges, only the Super User can actually manage the security policies provided by the TOE and the TOE offers a complete set of functions to facilitate effective management since the Super User allows for complete read-and-write access to the system.

4.4 Protection of the TSF

The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It

also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms (i.e., verification of the digital signature of each new image) so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

4.5 TOE Access

The TOE can be configured to display a message of the day banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

4.6 Trusted channels

The TOE protects interactive communication with administrators using SSHv2 for CLI access. In each case, both integrity and disclosure protection is ensured. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, the attempted connection will not be established.

The TOE protects communication with a log server and authentication server (TACACS+ and RADIUS) using TLS connections to prevent unintended disclosure or modification.

5 Assumptions

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

- collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (NDcPP21)

That information has not been reproduced here and the NDcPP21 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 NDcPP21 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 with a certain level of assurance (the assurance activities specified in the NDcPP21 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 NDcPP21 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- Configuration Guide, Extreme NetIron Configuration guide for Common Criteria NDcPP 2.1, 06.3.00aa, Supporting NetIron OS 06.3.00aa, August 2019

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 (NDcPP21) for Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa, Version 0.3, September 24, 2019 (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 a Common Criteria Certification document and ran the tests specified in the NDcPP21 including the tests associated with optional requirements.

9 Evaluated Configuration

The evaluated configuration is NetIron Family Devices with Multi-Service IronWare R06.3.00aa.

10 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 NetIron Family Devices with Multi-Service IronWare R06.3.00aa TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP21.

10.1 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 NetIron Family Devices with Multi-Service IronWare R06.3.00aa 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.

10.2 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 NDcPP21 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.

10.3 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.

10.4 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.

10.5 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 NDcPP21 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.

10.6 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.

The evaluator searched the National Vulnerability Database (NVD) from the NIST website to ensure no publicly known security flaws are identified for the TOE. The evaluator performed this search on August 13th, 2019. The following search terms were used:

- Extreme
- MLX
- IronWare
- NetIron
- Radius
- TACACS+
- SSH
- TLS

The public search for vulnerabilities did not uncover any residual vulnerability. 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.

10.7 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.

11 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 Common Criteria Supplemental User Guide. No versions of the TOE and software, either earlier or later were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the audit server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

12 Annexes

Not applicable

13 Security Target

The Security Target is identified as: *Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa (NDcPP21) Security Target, Version 0.4, September 9, 2019.*

14 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.

15 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 2.1, 24 September 2018 (NDcPP21)
- [5] Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa (NDcPP21) Security Target, Version 0.4, September 9, 2019 (ST).
- [6] Assurance Activity Report (NDcPP21) for Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.00aa, Version 0.3, September 24, 2019 (AAR).
- [7] Detailed Test Report (NDcPP21) for NetIron Family Devices with Multi-Service IronWare R06.3.00aa, Version 0.3, September 24, 2019 (DTR).
- [8] Evaluation Technical Report for Extreme Networks, Inc. NetIron Family Devices with Multi-Service IronWare R06.3.0aa, Version 0.3, September 24, 2019 (ETR)