Certification Report

EAL 3+ Evaluation of Extreme Networks ExtremeXOS Network Operating System v12.3.6.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-146-CR
Version:	1.0
Date:	28 March 2012
Pagination:	i to iii, 1 to 9

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI IT Security Evaluation & Test Facility located in Ottawa, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 28 March 2012, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria Portal (the official website of the Common Criteria Project).

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Disclaimer ..... **i**

Foreword ..... **ii**

Executive Summary **1**

1 Identification of Target of Evaluation **2**

2 TOE Description **2**

3 Evaluated Security Functionality **2**

4 Security Target **2**

5 Common Criteria Conformance **2**

6 Security Policy **3**

7 Assumptions and Clarification of Scope **3**

7.1 SECURE USAGE ASSUMPTIONS 3
7.2 ENVIRONMENTAL ASSUMPTIONS 3
7.3 CLARIFICATION OF SCOPE 4

8 Evaluated Configuration **4**

9 Documentation **5**

10 Evaluation Analysis Activities **5**

11 ITS Product Testing **6**

11.1 ASSESSMENT OF DEVELOPER TESTS 6
11.2 INDEPENDENT FUNCTIONAL TESTING 7
11.3 INDEPENDENT PENETRATION TESTING 7
11.4 CONDUCT OF TESTING 8
11.5 TESTING RESULTS 8

12 Results of the Evaluation **8**

13 Evaluator Comments, Observations and Recommendations **8**

14 Acronyms, Abbreviations and Initializations **8**

15 References **9**

Executive Summary

The Extreme Networks ExtremeXOS Network Operating System v12.3.6.2 (hereafter referred to as EXOS), from Extreme Networks, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

EXOS is network switching software, designed to provide network traffic management and control. The TOE runs on network switch appliances, it is designed specifically for the Extreme Networks Black Diamond and Summit network switches. It provides logical connections for management of network traffic flow and for management access. It is a software-only TOE.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 20 March 2012 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for EXOS, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 3 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3,* for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.* The following augmentation is claimed: ALC_FLR.2 – Flaw reporting procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the EXOS evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is Extreme Networks ExtremeXOS Network Operating System v12.3.6.2 (hereafter referred to as EXOS), from Extreme Networks, Inc.

2 TOE Description

EXOS is network switching software, designed to provide network traffic management and control. The TOE runs on network switch appliances, and is designed specifically for the Extreme Networks Black Diamond and Summit network switches. It provides logical connections for management of network traffic flow and for management access. It is a software-only TOE.

A detailed description of the EXOS architecture is found in Section 1.4.1 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for EXOS is identified in Section 1.4.3 of the ST.

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Extreme Networks, Inc. ExtremeXOS Network Operating System v12.3.6.2 Security Target
Version: 0.9
Date: 12 March 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

EXOS is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2; and
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

c. *Common Criteria EAL 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.2 – Flaw reporting procedures.

6 Security Policy

EXOS implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section 7 of the ST.

In addition, EXOS implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of EXOS should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The TOE administrators will periodically review the audit records generated by the TOE.
- The TOE will be placed in a network infrastructure such that information to be controlled will always flow through the TOE.
- The TOE does not have the ability to run general purpose applications and does not host public data.
- Only administrators have access to the administrative interfaces to ensure the network is secure.
- The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

7.3 Clarification of Scope

EXOS offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. EXOS is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for EXOS comprises the TOE running on the following appliances:

- BlackDiamond 8500/8800/8900 Series Switch
- Summit X150 Series
- Summit X250e Series
- Summit X350 Series
- Summit X450 Series
- Summit X450a Series
- Summit X450e Series
- Summit X650 Series
- SummitStack

Section 1.4 of the ST provides more details about the evaluated configuration and architecture.

The publication entitled: Extreme Networks, Inc. ExtremeXOS Network Operating System v12.3.6.2 Guidance Documentation Supplement, v0.7 describes the procedures necessary to install and operate EXOS in its evaluated configuration.

9 Documentation

The following Extreme Networks, Inc. documents provided to the consumer are as follows:

a. Summit Family Switches Hardware Installation Guide, Summit x150, x250e, x350, x450, x450a, x450e, x650 Series, SummitStack, Published: July 2011, Part Number: 100286-00 Rev. 12;

b. BlackDiamond 8800 Series Switches Hardware Installation Guide, BlackDiamond 8806 Switch, BlackDiamond 8810 Switch, Published: July 2011, Part Number: 100284-00 Rev. 12;

c. ExtremeXOS Concepts Guide, Software Version 12.3, Published: August 2009, Part Number: 100339-00 Rev. 02;

d. ExtremeXOS Command Reference Guide, Software Version 12.3, Published: August 2009, Part Number: 100340-00 Rev. 02; and

e. Extreme Networks, Inc. ExtremeXOS Network Operating System v12.3.6.2 Guidance Documentation Supplement, v0.7

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of EXOS, including the following areas:

Development: The evaluators analyzed the EXOS functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the EXOS security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the EXOS preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the EXOS configuration management system and associated documentation was performed. The evaluators found that the EXOS configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well-developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the EXOS design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of EXOS during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Extreme Networks, Inc. for EXOS. During a site visit, the evaluators examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of EXOS. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to EXOS in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

The evaluators analyzed the developer’s test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification and TOE design was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of CGI IT Security Evaluation & Test Facility test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Security Audit; The objective of this test goal is to verify that the audit functionality of the TOE works correctly with regards to logging authentication attempts and audit start-up/shutdown

c. Identification and authentication; the objective of this test goal is to verify that users are required to authenticate before taking any actions and that user accounts can be managed;

d. Data Flow Control; The objective of this test goal is to confirm that the Switch Flow Traffic Flow SFP can be properly implemented; and

e. Remote Management; The objective of this test goal is to demonstrate the TOE can be remotely managed by an authorized administrator via SNMP.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Attempting to bypass the flow control rules defined by the TOE ; and

b. Compromising the TSF and gaining access to VLAN traffic that should be inaccessible.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

EXOS was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at CGI IT Security Evaluation & Test Facility. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that EXOS behaves as specified in its ST and functional specification and TOE design.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The evaluator recommends that suitable protections are in place in the IT environment to secure any devices interacting with the TOE, such as TFTP, syslog and SNMP servers.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target

Acronym/Abbreviation/ Initialization	Description
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. Extreme Networks, Inc. ExtremeXOS Network Operating System v12.3.6.2 Security Target, 0.9, 12 March 2012

e. EAL3+ Common Criteria Evaluation of Extreme Networks, Inc. ExtremeXOS Network Operating System v12.3.6.2 Evaluation Technical Report (ETR), v1.0, 20 March 2012