Certification Report

EAL 4+ Evaluation of Crossbeam X-Series Platform with XOS v9.9.0 on X60 and X80-S Chassis

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-191-CR
Version: 1.0
Date: 03 July 2012
Pagination: i to iii, 1 to 10

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 EWA-Canada 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 03 July 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).

TABLE OF CONTENTS

Executive Summary

Crossbeam X-Series Platform with XOS v9.9.0 on X60 and X80-S Chassis (hereafter referred to as X-Series), from Crossbeam Systems, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

X-Series platform consolidates multiple security applications onto a single multifunction device. The applications that can be installed on the Crossbeam platform include antivirus, firewall, spam filtering, Intrusion Prevention System (IPS), proxy, and web content gateways. However, these applications were not included in the scope of this evaluation.

The platform is composed of a combination of hot-swappable modules seated on a common backplane. The modules provide processing and storage that is used to implement the functionality of the X-Series Operating System (XOS).

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 28 June 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 X-Series, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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 4 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 augmentations are claimed: ALC_FLR.2 – Flaw reporting procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the X-Series 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) 4 augmented evaluation is Crossbeam X-Series Platform with XOS v9.9.0 on X60 and X80-S Chassis (hereafter referred to as X-Series), from Crossbeam Systems, Inc.

2 TOE Description

X-Series platform consolidates multiple security applications onto a single multifunction device. The applications that can be installed on the Crossbeam platform include antivirus, firewall, spam filtering, Intrusion Prevention System (IPS), proxy, and web content gateways.

The platform is composed of a combination of hot-swappable modules seated on a common backplane. The modules provide processing and storage that is used to implement the functionality of the X-Series Operating System (XOS).

A detailed description of the X-Series architecture is found in Section 1.5 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for X-Series is identified in Section 1.5 of the ST.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
X60 and X80-S Platforms	*Pending* [2]

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in X-Series:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	1220, 1221
Advanced Encryption Standard (AES)	FIPS 197	1877, 1878
Rivest Shamir Adleman (RSA)	FIPS 186-2	958, 961
Secure Hash Algorithm (SHA-1)	FIPS 180-2	1650, 1651

[2] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

Cryptographic Algorithm	Standard	Certificate #
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	1121, 1122
Digital Signature Algorithm (DSA)	FIPS 186-2	587, 590
Pseudo Random Number Generation (PRNG)	ANSI x93.1	983, 986

4 Security Target

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

Title: Crossbeam Systems, Inc. X-Series Platform with XOS v9.9.0 on X60 and X80-S
Version: 0.10
Date: 26 June 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*.

X-Series is:

a. *Common Criteria Part 2 extended;* with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - FCS_COMM_PROT_EXT.1 - Communications Protection
    - FCS_RBG_EXT.1 - Cryptographic Operation (Random Bit Generation)
    - FIA_PMG_EXT.1 - Password Management
    - FIA_UAU_EXT.5 - Password-based Authentication Mechanism
    - FIA_UAU_EXT.7 - Protected Authentication Feedback
    - FPT_PTD.1 - Management of TSF Data (for reading authentication data)
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 4 augmented*, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.2 – Flaw reporting procedures.

6 Security Policy

X-Series 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 7.1 of the ST.

In addition, X-Series implements policies pertaining to security audit, cryptographic support, user data protection, identification and authentication, security management, protection of the TSF, resource utilization, and TOE access. Further details on these security policies may be found in Section 7.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of X-Series 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:

- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains; and
- The administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is located within a controlled access facility;
- The TOE environment provides the network connectivity required to allow the TOE to perform its intended function; and
- The TOE environment should provide protection to ensure that Network Time Protocol (NTP) information communicated from an NTP source to the TOE cannot be modified by an attacker.

7.3 Clarification of Scope

X-Series offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. X-Series 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 X-Series comprises:

- XOS software v9.9.0,
- CPM blades,
- APM blades,
- NPM blades,
- Carrier-grade X60 and X80-S chassis.

The following publications describe the procedures necessary to install and operate X-Series in its evaluated configuration:

- Crossbeam XOS Configuration Guide, Jan 2012;
- Crossbeam Multi-System High Availability Configuration Guide, Jan 2012;
- Crossbeam XOS 9.9.0 running on X60 and X80 Platforms Guidance Supplement v0.4;
- FIPS 140-2 and Common Criteria Administration Guide for Crossbeam® X-Series Platforms April 2012;
- X60 Platform Hardware Installation Guide, Jan 2012; and
- X80-S Platform Hardware Installation Guide, Jan 2012

9 Documentation

The Crossbeam Systems, Inc. documents provided to the consumer are as follows:

a. Crossbeam XOS Configuration Guide, Jan 2012;

b. Crossbeam Multi-System High Availability Configuration Guide, Jan 2012;

c. Crossbeam XOS 9.9.0 running on X60 and X80 Platforms Guidance Supplement v0.4;

d. FIPS 140-2 and Common Criteria Administration Guide for Crossbeam® X-Series Platforms April 2012;

e. X60 Platform Hardware Installation Guide, Jan 2012;

f. X80-S Platform Hardware Installation Guide, Jan 2012

g. Crossbeam XOS Command Reference Guide Jan 2012; and

h. Crossbeam XOS 9.9.0 Release Notes April 2012.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of X-Series, including the following areas:

Development: The evaluators analyzed the X-Series functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the X-Series security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the X-Series 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 X-Series configuration management system and associated documentation was performed. The evaluators found that the X-Series configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorized access to the configuration items.

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

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the X-Series design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Crossbeam Systems, Inc. for X-Series. During a site visit, the evaluators also 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 X-Series. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to X-Series in its operational environment.

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

11 ITS Product Testing

Testing at EAL 4 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[3].

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, TOE design and security architecture description 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 EWA-Canada test goals:

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

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

b. User access: The objective of this test goal is to exercise the I&A and security management functionality of the TOE with regard to users.

11.3 Independent Penetration Testing

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

a. Port scanning: The objective of this test goal was to scan the TOE using a port scanner to determine what ports were open and what services were running; and

b. Vulnerability scanning: The objective of this test goal is to scan the TOE using a vulnerability scanner to determine if the TOE is susceptible to any particular attacks.

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

11.4 Conduct of Testing

X-Series 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 EWA-Canada and at the developer site. 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 X-Series behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

It is recommended that the TOE remain in the FIPS-mode of operation as this was the evaluated configuration and provides for a locked down and secure environment. Without this extra security, it is in a non-tested configuration and could lead to security vulnerabilities in the day to day operation of the TOE.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
APM	Application Processor modules
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CPM	Control Processor Modules
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NPM	Network Processor Modules
PALCAN	Program for the Accreditation of Laboratories - Canada
ST	Security Target
TOE	Target of Evaluation
XOS	X-Series Operating System

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. Crossbeam Systems, Inc. X-Series Platform with XOS v9.9.0 on X60 and X80-S, 0.10, 26 June 2012.

e. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of Crossbeam Systems, Inc. X-Series Platform with XOS v9.9.0, Version 1.1, 28 June 2012.