Certification Report

EAL 4+ Evaluation of WatchGuard XCS v9.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-161-CR
Version:	1.0
Date:	20 April 2012
Pagination:	i to iii, 1 to 8

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 20 April 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).

This certification report makes reference to the following registered trademark:

- WatchGuard is a registered trademark of WatchGuard Technologies, Inc. in the United States and/or other countries.

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

TABLE OF CONTENTS

Executive Summary

WatchGuard XCS v9.2 (hereafter referred to as XCS v9.2), from WatchGuard Technologies, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

XCS v9.2 is a software application that runs on WatchGuard XCS appliances[1] providing corporations with an enterprise-class email security, privacy and compliance solution that protects against inbound threats, and controls outbound information to prevent data loss.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 21 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 XCS v9.2, 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)[2] 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 augmentation is claimed: ALC_FLR.2 – Basic Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the XCS v9.2 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] WatchGuard XCS appliance models: XCS 170, 370, 570, 770R, 970, and 1170.

[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.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is WatchGuard XCS v9.2 (hereafter referred to as XCS v9.2), from WatchGuard Technologies, Inc.

2 TOE Description

XCS v9.2 is a software application that runs on WatchGuard XCS appliances[3] providing corporations with an enterprise-class email security, privacy and compliance solution that protects against inbound threats, and controls outbound information to prevent data loss.

A detailed description of the XCS v9.2 architecture is found in Section 1.4 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for XCS v9.2 is identified in Section 6 of the ST.

4 Security Target

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

Title: WatchGuard XCS v9.2 Security Target
Version: 1.9
Date: 8 December 2011

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.*

XCS v9.2 is:

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

[3] WatchGuard XCS appliance models: XCS 170, 370, 570, 770R, 970, and 1170.

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 - Basic Flaw Reporting Procedures.

6 Security Policy

XCS v9.2 implements access control and flow control policies. Details on these security policies may be found in Section 6.2.5 of the ST.

In addition, XCS v9.2 implements policies pertaining to security audit, user data protection, identification and authentication, security management, and protection of TOE security functions. Further details on these security policies may be found in Section 1.4.2 of the ST.

7 Assumptions and Clarification of Scope

Consumers of XCS v9.2 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 system administrator will adhere to the secure guidance provided for the operation of the TOE; and

- The users of the internal network from which administration of the TOE is performed are trusted neither willfully hostile to the TOE, nor will intercept network traffic or open up the trusted network by introducing any uncontrolled connections to untrusted networks.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE will be physically protected to prevent hostile individuals engaging in theft, implantation of devices, or unauthorized alteration of the physical configuration of the mail server;

- All SMTP email traffic between networks connected to the TOE will be transferred through the TOE; and

- The TOE environment is appropriately scalable to provide support to the IT Systems in the organization it is deployed.

7.3 Clarification of Scope

XCS v9.2 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. XCS v9.2 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 XCS v9.2 comprises XCS v9.2 running on WatchGuard XCS appliance models: XCS 170, 370, 570, 770R, 970, and 1170. Further detail may be found in Section 1.4 of the Security Target (ST).

9 Documentation

The WatchGuard Technologies, Inc. documents provided to the consumer are as follows:

a. Release Notes: WatchGuard XCS v9.2 Release Notes - June 14, 2011;

b. Preparatory Guide: WatchGuard XCS Preparatory Guide - v1.2;

c. User Guide: WatchGuard XCS v9.2 User Guide - 6/15/2011;

d. Field Guide: WatchGuard XCS v9.2 Field Guide - 6/13/11;

e. Hardware Guide: WatchGuard XCS Hardware Guide - 170, 370, 570, 770 and 770R models - P.N. 275-3727-003;

f. Hardware Guide: WatchGuard XCS Hardware Guide - 970 and 1170 models - P.N. 275-3728-001;

g. Quick Start Guide: WatchGuard XCS Quick Start Guide - 170, 370, 570, 770 and 770R models - P.N. 352-3707-003; and

h. Quick Start Guide: WatchGuard XCS Quick Start Guide - 970 and 1170 models - P.N. 352-3708-002.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of XCS v9.2, including the following areas:

Development: The evaluators analyzed the XCS v9.2 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 XCS v9.2 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 XCS v9.2 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 XCS v9.2 configuration management system and associated documentation was performed. The evaluators found that the XCS v9.2 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 unauthorised 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 XCS v9.2 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 XCS v9.2 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 WatchGuard Technologies, Inc. for XCS v9.2. 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 XCS v9.2. 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 XCS v9.2 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[4].

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;

b. Authentication: The objective of this test goal is to confirm that the administrator must authenticate using a web browser or the system console before being allowed access to any TSF-mediated actions;

c. Audit: The objective of this test goal is to confirm that the TOE generates audit records for login failures, and provides a review mechanism for administrators;

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

d. Backup and Restore: The objective of this test goal is to confirm that the TOE provides the administrator with the capability to create backups to a USB Drive and that a restore can be performed; and

e. Alarms: The objective of this test goal is to confirm that alarms are generated, logged, and can be reviewed.

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 port scanning, cross site scripting[5], and attempts to cause the TOE to run scripts embedded in messages.

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

11.4 Conduct of Testing

XCS v9.2 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. 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 XCS v9.2 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 Acronyms, Abbreviations and Initializations

[5] Cross-site scripting (XSS) is a type of vulnerability that enables attackers to inject client-side script into web pages viewed by other users.

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
ST	Security Target
TOE	Target of Evaluation
XCS	Extensible Content Security

14 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. WatchGuard XCS v9.2 Security Target, Version: 1.9, 8 December 2011.

e. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of WatchGuard Technologies, Inc. WatchGuard XCS Server v9.2 Document No. 1662-000-D002, v1.4, 21 March 2012.