Certification Report

EAL 2+ Evaluation of Trustwave WebDefend Enterprise Software Version 5.1 SP1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-226-CR
Version:	1.0
Date:	22 January 2013
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 EWA-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 08 January 2013, 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

Executive Summary

Trustwave WebDefend Enterprise Software Version 5.1 SP1 (hereafter referred to as WebDefend 5.1), from Trustwave Holdings, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

WebDefend 5.1 is a software TOE which monitors web application traffic, detects security events, and responds to those events according to configured policies.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 20 December 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 WebDefend 5.1, 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 2 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 WebDefend 5.1 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) 2 augmented evaluation is Trustwave WebDefend Enterprise Software Version 5.1 SP1 (hereafter referred to as WebDefend 5.1), from Trustwave Holdings, Inc..

2 TOE Description

WebDefend 5.1 is a software TOE which monitors web application traffic, detects security events, and responds to those events according to configured policies. The list below provides a brief description of the TOE components.

- **WebDefend Sensor Application.** The WebDefend Sensor Application monitors the web applications being protected, analyzes HTTP traffic and generates events, performs the behavioral learning and web application profile building, and executes the configured actions upon event detection;

- **WebDefend Manager**. The WebDefend Manager distributes configuration updates to the Sensor application. This component provides the interface for insertion and retrieval of audit records, configuration information, System data and reports.

- **WebDefend Watchdog.** The WebDefend Watchdog monitors the WebDefend Sensor Application to ensure it is functioning correctly.

- **WebDefend Reporting Service.** The WebDefend Reporting Service is responsible for generating the configured WebDefend reports.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for WebDefend 5.1 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: Trustwave WebDefend Enterprise Software Security Target
Version: 1.5
Date: 22 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.*

WebDefend 5.1 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:
   - IDS_SDC.1 - System Data Collection;
   - IDS_ANL.1 - Analyser Analysis;
   - IDS_RCT.1 - Analyser React;
   - IDS_RDR.1 -Restricted Data Review;
   - IDS_STG.1 - System Data Storage;
   - IDS_STG.1 - Guarantee of System Data Availability; and
   - IDS_STG.2 - Prevention of System Data Loss.

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

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

6 Security Policy

WebDefend 5.1 implements a restricted data review policy which restricts access to alert and event information collected by the TOE to authorized administrators. Details of this policy can be found in Section 6 of the ST.

In addition, WebDefend 5.1 implements policies pertaining to security audit, identification and authentication, security management and intrusion detection. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of WebDefend 5.1 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 has access to all the IT System data it needs to perform its functions.
- The TOE is appropriately scalable to the IT System the TOE monitors.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.
- The TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.

7.3 Clarification of Scope

WebDefend 5.1 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. WebDefend 5.1 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 WebDefend 5.1 comprises WebDefend software version 5.1 build 7.11.033-3.1 executing on a dedicated appliance (GX30i, GX60i, GX110i, GX120i) along with the WebDefend console application version 5.1 build 7.11.033 executing on a Windows workstation running Microsoft Windows XP (SP3 or higher), Microsoft Windows 2003 (32 bit or 64 bit) (any SP level), Microsoft Windows 2008 (32 bit or 64 bit) (any SP level), Microsoft Windows Vista (32 bit or 64 bit) (SP2 or higher), Microsoft Windows 2008 (32 bit or 64 bit) (any SP level), Microsoft Windows 7 (32 bit or 64 bit) (SP1 or higher).

The publication entitled *Trustwave WebDefend Version 5.1 Common Criteria Supplement* describes the procedures necessary to install and operate WebDefend 5.1 in its evaluated configuration.

9 Documentation

In support of WebDefend 5.1, Trustwave Holdings, Inc. provides the following documents to the consumer:

a. Trustwave WebDefend Version 5.1 Getting Started Guide Version 5.1, December 2011

b. Trustwave WebDefend Version 5.1 User Guide Version 5.1, June 2011

c. Trustwave WebDefend Version 5.1 Common Criteria Supplement Version 5.1, July 2012

d. Trustwave WebDefend V4.5 to V5.1 Upgrade Instructions Version 1.1, March 2012

e. Trustwave WebDefend V5.0 to V5.1 Upgrade Instructions Version 1.1, March 2012

f. Trustwave WebDefend V5.1 to V5.1SP1 Upgrade Instructions Version 1.0, June 2012

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of WebDefend 5.1, including the following areas:

Development: The evaluators analyzed the WebDefend 5.1 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 WebDefend 5.1 security architectural description and determined that the initialization process is secure, 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 WebDefend 5.1 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 WebDefend 5.1 configuration management system and associated documentation was performed. The evaluators found that the WebDefend 5.1 configuration items were clearly marked. The developer’s configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of WebDefend 5.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the WebDefend 5.1. 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 WebDefend 5.1. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify WebDefend 5.1 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to WebDefend 5.1 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 2 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].

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

[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.

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. Identification and Authentication: The objective of this test goal is test the verification of user attributes and identification and authentication of TOE users.

c. Security Management: The objective of this test goal is to confirm the TOE's ability to maintain security attributes for various administrative roles.

d. Audit: The objective of this test goal is to verify the TOE’s audit functionality and confirm that the TOE can protect stored audit records from unauthorized deletion.

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. Port Scan: The objective of this test goal is to scan the TOE using a port scanner to determine any potential vulnerabilities;

b. Vulnerability Identification: Tool Scanning: The objective of this test goal is to scan the TOE for vulnerabilities using automated tools;

c. Information Leakage Verification: The objective of this test goal is to monitor the TOE for leakage during start-up, shutdown, login, and other scenarios using a packet sniffer; and

d. Privilege escalation: The objective of this test goal is to confirm that the TOE is not vulnerable to the privilege escalation attack uncovered during the public domain search.

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

11.4 Conduct of Testing

WebDefend 5.1 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 WebDefend 5.1 behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ 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

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
TOE	Target of Evaluation

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. Trustwave WebDefend Enterprise Software Security Target, version 1.5, 22 June 2012.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of Trustwave Holdings, Inc. WebDefend Enterprise Software version 5.1, v1.0 20 December 2012.