Certification Report

Trustwave DbProtect Version 6.4.3

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-308-CR
Version: 1.0
Date: 21 July 2015
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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies 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, 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, 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.

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 21 July 2015, 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

Trustwave DbProtect Version 6.4.3 (hereafter referred to as DbProtect Version 6.4.3), from Trustwave Holdings, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that DbProtect Version 6.4.3 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

DbProtect Version 6.4.3 is a database vulnerability assessment and monitoring suite that helps to identify vulnerable databases residing within the network by scanning for potential security vulnerabilities within those databases and monitoring activity by users with them.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 21 July 2015 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 DbProtect Version 6.4.3, and the security functional/assurance 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.

Communications Security Establishment, as the CCS Certification Body, declares that the DbProtect Version 6.4.3 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 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is Trustwave DbProtect Version 6.4.3 (hereafter referred to as DbProtect Version 6.4.3), from Trustwave Holdings, Inc..

2 TOE Description

DbProtect Version 6.4.3 scans, and monitors databases for vulnerabilities and suspicious behavior. Scans are performed to proactively detect vulnerabilities, misconfigurations, and inappropriate permission settings. Monitoring is performed to react to unusual or suspicious behavior and alerts may be generated for configured conditions.

The TOE comprises a single management console component, one or more database scanning engines and one or more sensors. Each of these components is an application designed to run in the context of a general purpose operating system. The console presents the administrative interface that centralizes the management of multiple scan engines and sensors. The console also provides access to the data collected by the scan engines and alerts generated by the sensors.

3 Security Policy

DbProtect Version 6.4.3 implements a role-based access control policy to control administrative access to the system. In addition, DbProtect Version 6.4.3 implements policies pertaining to the following security functional classes:

- *Identification and Authentication*
- *Security Management*
- *Intrusion Detection*

4 Security Target

The ST associated with this Certification Report is identified below:

Trustwave DbProtect Version 6.4.3 Security Target, Version 1.8, July 21, 2015

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

DbProtect Version 6.4.3 is:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures

b. *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 – System Analysis*
    - *IDS_RDR.1 – Restricted Data Review*
    - *IDS_RCT.1 – System React*

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

6 Assumptions and Clarification of Scope

Consumers of DbProtect Version 6.4.3 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *The TOE will be managed in a manner that allows it to appropriately address changes in the database 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.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE has access to all the database data it needs to perform its functions.*
- *The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical and logical access.*

7 Evaluated Configuration

The evaluated configuration for DbProtect Version 6.4.3 comprises the DbProtect Version 6.4.3 application running on Windows Server 2012. The TOE requires a Microsoft SQL Server 2012 database in the operational environment for the storage of TOE configuration and scan results. The TOE performed scans on the following DBMSs:

- *Oracle 11gR1, 11gR2;*
- *Microsoft SQL Server 2012;*
- *Sybase ASE 15.0, 15.5, 15.7;*
- *IBM DB2 LUW 9.1, 9.5, 9.7, 10.1;*
- *MySQL 5.1, 5.5; and*
- *Hadoop 1.*

The publication entitled Trustwave DbProtect V6.4.3 Common Criteria Supplement, Version 1.2, July 10, 2015 describes the procedures necessary to install and operate DbProtect Version 6.4.3 in its evaluated configuration.

8 Documentation

The Trustwave Holdings, Inc. documents provided to the consumer are as follows:

a. Trustwave DbProtect 6.4 Series User Guide, October 2012;

b. Trustwave DbProtect 6.4 Series Sensor Guide, June 2012;

c. Trustwave DbProtect 6.4.3 Getting Started Guide, December 2013; and

d. Trustwave DbProtect V6.4.3 Common Criteria Supplement, Version 1.2, July 10, 2015

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of DbProtect Version 6.4.3, including the following areas:

Development: The evaluators analyzed the DbProtect Version 6.4.3 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 DbProtect Version 6.4.3 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 DbProtect Version 6.4.3 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 DbProtect Version 6.4.3 configuration management system and associated documentation was performed. The evaluators found that the DbProtect Version 6.4.3 configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of DbProtect Version 6.4.3 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the DbProtect Version 6.4.3. 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.

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

10 ITS Product Testing

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

10.1 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[1].

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.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

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 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. Sensor Alert Text File: The objective of this test goal is to confirm that the TOE can log alert information to a separate text file;

c. Concurrent Users: The objective of this test goal is to confirm that only one concurrent user can actively run the TOE; and

d. Database Credential Testing: The objective of this test goal is to confirm that only users with appropriate database credentials can initiate a scan of a database.

10.3 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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities; and

b. Information Leakage: The objective of this test goal is to attempt to capture packets between the TOE and the remote scanned databases in an attempt to determine login or password information.

[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.

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

10.4 Conduct of Testing

DbProtect Version 6.4.3 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that DbProtect Version 6.4.3 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 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
TSF	TOE Security Function

13 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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Trustwave DbProtect Version 6.4.3 Security Target, Version 1.8, July 21, 2015.

e. Evaluation Technical Report for Trustwave Holdings, Inc. DbProtect Version 6.4.3, Document No. 1860-000-D002, Version 1.0, 21 July 2015.