Certification Report

McAfee® Database Security 4.4

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment Canada, 2013

Document number: 383-4-245-CR
Version: 1.2
Date: 16 September 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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 and test facility.

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 16 September 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).

This certification report makes reference to the following trademarks or registered trademarks:

- McAfee is a registered trademark of McAfee, Inc.

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

TABLE OF CONTENTS

Executive Summary

McAfee® Database Security 4.4 (hereafter referred to as DB Sec 4.4), from McAfee, Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

DB Sec 4.4 is a software solution that monitors a Database Management System (DBMS) and protects it from both internal and external threats. The TOE provides full visibility into DBMS user and application activity by way of analysis of SQL statements and queries interacting with the DBMS. Analysis of DBMS transactions is determined by a monitoring policy consisting of a set of rules (predefined and/or custom) which are configured to issue alerts and/or terminate suspicious activities. The TOE can be used in support of simple, single DBMS installations as well as complex, multi-server, multi-DBMS installations.

CGI IT security evaluation and test facility is the CCEF that conducted the evaluation. This evaluation was completed on 23 July 2013 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 DB Sec 4.4, 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.* The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the DB Sec 4.4 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 McAfee® Database Security 4.4 (hereafter referred to as DB Sec 4.4), from McAfee, Inc..

2 TOE Description

DB Sec 4.4 is a software solution that monitors a Database Management System (DBMS) and protects it from both internal and external threats. The TOE provides full visibility into DBMS user and application activity by way of analysis of SQL statements and queries interacting with the DBMS. Analysis of DBMS transactions is determined by a monitoring policy consisting of a set of rules (predefined and/or custom) which are configured to issue alerts and/or terminate suspicious activities. The TOE can be used in support of simple, single DBMS installations as well as complex, multi-server, multi-DBMS installations.

A detailed description of the DB Sec 4.4 architecture is found in Section 1.6 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for DB Sec 4.4 is identified in Section 6 of the ST.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in DB Sec 4.4:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	1014 / 1017
Advanced Encryption Standard (AES)	FIPS 197	1544 / 1547
Rivest Shamir Adleman (RSA)	ANSI X9.31 PKCS #1 v1.5 RSASSA-PSS	747 / 752
Digital Signature Algorithm (DSA)	FIPS 186-3	476 / 479
Secure Hash Algorithm (SHA-1)	FIPS 180-2	1369 / 1374
Random Number Generator (RNG))	ANSI X9.31	832 / 836

4 Security Target

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

Title: McAfee Database Security 4.4
Version: 1.4
Date: 18 June 2013

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.*

DB Sec 4.4 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 – Analyzer Analysis;
   - IDS_RDR.1 – Restricted Data Review;
   - IDS_RCT.1 - Analyzer React;
   - 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: e.g. ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

DB Sec 4.4 implements a role-based access control policy to control user access to the system and its data; details of this security policy can be found in Section 6 of the ST.

In addition, DB Sec 4.4 implements insert other policies pertaining to security audit, cryptographic support, identification and authentication, security management and protection of the TSF. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of DB Sec 4.4 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 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; and
- The TOE can only be accessed by authorized users.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE has access to all the IT System data it needs to perform its functions;
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors;
- The TOE is appropriately scalable to the IT System the TOE monitors;
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification; and
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

7.3 Clarification of Scope

DB Sec 4.4 incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

8 Evaluated Configuration

The evaluated configuration for DB Sec 4.4 is software only and comprises:

McAfee Database Security Version 4.4, comprising of the following licensed software:

- McAfee Database Activity Monitoring Version 4.4, including:
  - McAfee Database Security Server;
  - McAfee Database Security Sensor; and
  - McAfee Database Security Web Console;
- McAfee Vulnerability Manager for Databases Version 4.4; and
- McAfee Virtual Patching for Databases Version 4.4.

The Database Security Software is installed on a GPC running one of the following Operating Systems:

- Windows Server 2008 R2 Enterprise with Service Pack 1;
- Windows Server 2008 R2 Standard with Service Pack 1; or
- Windows Server 2008 R2 Datacenter with Service Pack 1.

McAfee Database Security Sensor is supported on the following DBMS:

- MS-SQL 2005
- MS-SQL 2008

The publication entitled Operational User Guidance and Preparative Procedures Supplement: McAfee Database Security 4.4.3 Document Version 1.1, May 20, 2013 describes the procedures necessary to install and operate DB Sec 4.4 in its evaluated configuration.

9 Documentation

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

a. McAfee Database Security Installation Guide (4.3.0) Document Version 1.0, February 2012;

b. McAfee Database Security User's Guide (4.4.0) Document Version 1.1, June 2012; and

c. Operational User Guidance and Preparative Procedures Supplement: McAfee Database Security 4.4.3 Document Version 1.1, May 20, 2013.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of DB Sec 4.4, including the following areas:

Development: The evaluators analyzed the DB Sec 4.4 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 DB Sec 4.4 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 DB Sec 4.4 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 DB Sec 4.4 configuration management system and associated documentation was performed. The evaluators found that the DB Sec 4.4 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 DB Sec 4.4 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the DB Sec 4.4. 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 DB Sec 4.4. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify DB Sec 4.4 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to DB Sec 4.4 in its operational environment.

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

11 ITS Product Testing

Testing 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.

[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.

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 and 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. Sensor detects Malicious code: The objective of this test goal is to ensure the Sensor will detect malicious SQL code and react as per SFRs in ST ;

c. Detect malicious activity through statistical analysis: The objective of this test goal is to verify that the management system along with sensor detects malicious activity through statistical analysis of data; and

d. Capture Database vulnerability during a VA (Vulnerability Assessment) scan: The objective of this test goal is to confirm that a VA scan will capture a vulnerability defined for the VA test.

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. Attempt to bypass sensor capture with large malicious commands: The objective of this test goal is to verify that the sensor is capable of detecting malicious commands even when large queries in rapid succession are run;

b. Attempt to bypass Disconnect and Quarantine rules: The objective of this test goal is to demonstrate that a remote DBMS user cannot bypass the TOE rules;

c. Web Based User Interface: The objective of this test goal is to analyze the web based TSFI (TOE Security Functionality Interface) for vulnerabilities; and

d. Malformed and Obfuscated Data: The objective of this test goal is to gain assurance that the sensors can deal with malformed and obfuscated data without breaking down.

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

11.4 Conduct of Testing

DB Sec 4.4 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 and 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 DB Sec 4.4 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 Evaluator Comments, Observations and Recommendations

It is strongly recommended that the end customer obtain a copy of the "Operational User Guidance and Preparative Procedures Supplement" document to understand the evaluation configuration so that the TOE shall be configured in an evaluated and secure way.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DBMS	Database Management System
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IDS	Intrusion Detection System
IT	Information Technology
ITSET	Information Technology Security Evaluation

Acronym/Abbreviation/ Initialization	Description
	and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
RNG	Random Number Generator
RSA	Rivest Shamir Aldeman
SFR	Security Functional Requirement
SHA-1	Secure hash Algorithm
ST	Security Target
SQL	Structured Query Language
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
VA	Vulnerability Assessment

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 4, September 2012.

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

d. McAfee Database Security 4.4, version 1.4, 18 June 2013 Security Target.

e. ETR McAfee Database Security 4.4, version 2.0, 23 July 2013.