Certification Report

EAL 2+ Evaluation of SenSage 4.6.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-141-CR
Version: 1.1
Date: 9 September 2011
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 DOMUS ITSL located in Ottawa, Ontario.

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 9 September 2011, 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

The SenSage 4.6.2 (hereafter referred to as SenSage), from SenSage, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2+ augmented with Flaw Remediation (ALC_FLR.1) evaluation.

SenSage is an Event Data Warehouse solution that handles log and event data. Event data contains evidence directly pertaining to and resulting from the execution of a business process or system function.

When properly configured, the Event Data Warehouse contains the records of system activities such as users logging in and logging out, users accessing confidential files, activities on the firewall, emails being sent and received, information on processed transactions, and the web sites being accessed.

DOMUS ITSL is the CCEF that conducted the evaluation. This evaluation was completed on 15 July 2011 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 SenSage, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the 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.1 – Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that SenSage 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 SenSage 4.6.2 (hereafter referred to as SenSage), from SenSage, Inc..

2 TOE Description

SenSage is an Event Data Warehouse solution that handles log and event data. Event data contains evidence directly pertaining to and resulting from the execution of a business process or system function.

When properly configured, the Event Data Warehouse contains the records of system activities such as users logging in and logging out, users accessing confidential files, activities on the firewall, emails being sent and received, information on processed transactions, and the web sites being accessed.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for SenSage is identified in Section 7 of the Security Target (ST).

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

Cryptographic Module	**Certificate #**
CryptoCore Module	*Pending* [2]

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in SenSage:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	*Pending*
Advanced Encryption Standard (AES)	FIPS 197	*Pending*
Random Number Generation	ANSI X9.31	*Pending*

[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.

4 Security Target

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

Title: SensSage 4.6.2 Security Target
Version: 1.2
Date: 07 July 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.

SenSage 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:
   - EXT_FAU_EDC.1 and
   - EXT_FAU_SAA.1
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.1 – Basic* Flaw Remediation

6 Security Policy

SenSage implements a role-based access control policy to control user access to the system.

In addition, SenSage implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the SenSage 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 Assumption is listed in the ST:

- The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE resides in a physically controlled access facility that prevents unauthorized physical access; and

- The IT environment provides the TOE with the necessary reliable timestamps.

8 Evaluated Configuration

The evaluated configuration comprises the software application SenSage 4.6.2 configured and running on the platforms identified in Section 1.4.2 of the ST.

The publication entitled *SenSage Installation, Configuration, and Upgrade Guide 4.6.2, January 26, 2011* describes the procedures necessary to install and operate SenSage in its evaluated configuration.

9 Documentation

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

- SenSage Administration Guide 4.6.2, January 26, 2011;
- SenSage Analytics Guide 4.6.2, January 26, 2011;
- SenSage Event Collection Guide 4.6.2, January 27, 2011;
- SenSage Event Processing Language Developers Guide Version 4.6.2, January 26, 2011;
- SenSage Reporting Guide 4.6.2, January 26, 2011;
- SenSage Release Notes 4.6.2, January 26, 2011;
- SenSage Installation, Configuration, and Upgrade Guide 4.6.2, January 26, 2011;
- SenSage, Inc. SenSage 4.6.2 Guidance Documentation Supplement v0.4;
- SenSage, Inc. SenSage 4.6.2 Security Target v1.2;
- SenSage Third-Party Open Source Licensing, January 26, 2011;
- Check Point LEA (Log Export API) Specification OPSEC SDK 6.0 May 2006;
- Java™ Network Launching Protocol and API Specification, v6.0; and
- SenSage 4.6 SLS Errors.txt.

10 Evaluation Analysis Activities

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

Development: The evaluators analyzed the SenSage functional specification, design documentation; 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 SenSage security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the SenSage 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 SenSage configuration management system and associated documentation was performed. The evaluators found that the SenSage 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 SenSage during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for TOE short name. 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 SenSage. 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 the SenSage 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[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 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 was the following list of DOMUS ITSL test goals:

a. Repeat of Developer's Tests: The evaluator repeated all the developer tests to gain a deeper understanding of the TOE and the TOE interfaces. All security functions and interfaces were exercised;

b. Security Audit: The objective of this test goal is to determine the TOE's ability to audit the activity of users;

c. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data;

d. Identification and Authentication: The objective of these tests is to ensure that access to the TOE is restricted to authorized administrators only; and

e. Security Management: The objective of these tests is to ensure that authorized individuals are able to manage the TOE in a secure manner.

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:

[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.

- Reconnaissance and exploratory testing to observe application behavior including client side script and HTTP packet inspection using Firecookie and Wireshark;
- Use of automated vulnerability scanning tools (NESSUS and NMAP) to discover potential network, platform and application layer vulnerabilities;
- Capture and analysis of session keys to determine susceptibility to prediction; and
- Penetration attempts involving manipulation of client side variables.

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

11.4 Conduct of Testing

SenSage 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 DOMUS ITSL. 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 SenSage 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

Consumers should review the security aspects of the intended environment (defined in Section 4.2 of the ST) and the excluded functionality (detailed in Section 1.5.1 of the ST) when deploying SenSage.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
3DES	Triple-DES
AES	Advanced Encryption Standard

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
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

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. SensSage 4.6 Security Target, v0.9, 1.2, 07 July 2011.

e. SenSage 4.6.2 Evaluation Technical Report v1.0, 15 July 2011-09-08.