Certification Report

EAL 3+ Evaluation of RSA enVision® platform v4.0 SP 1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-118-CR
Version: 1.0
Date: 22 January 2010
Pagination: i to iii, 1 to 11

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 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. 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, 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 22 January 2010, 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 RSA enVision® platform v4.0 SP 1 (hereafter referred to as RSA enVision), from RSA, The Security Division of EMC, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 *augmented* evaluation.

RSA enVision is a security information event management (SIEM) and log management solution, capable of collecting and analyzing large amounts of data in real-time from an array of event sources. It provides a log management solution for simplifying compliance, enhancing security and risk mitigation, and optimizing IT and network operations through the automated collection, analysis, alerting, auditing, reporting, and security storage of all logs.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 11 December 2009 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 RSA enVision, 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 3 *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 2*. The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the RSA enVision 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) 3 *augmented* evaluation is RSA enVision® platform v4.0 SP 1 (hereafter referred to as RSA enVision), from RSA, The Security Division of EMC.

2 TOE Description

RSA enVision is a security information event management (SIEM) and log management solution, capable of collecting and analyzing large amounts of data in real-time from an array of event sources. It provides a log management solution for simplifying compliance, enhancing security and risk mitigation, and optimizing IT and network operations through the automated collection, analysis, alerting, auditing, reporting, and security storage of all logs.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for RSA enVision is identified in Section 6 (Security Requirements) of the Security Target (ST).

4 Security Target

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

Title: RSA, The Security Division of EMC enVision® platform v4.0 SP 1 Security Target
Version: 0.8
Date: 11 December 2009

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.*

RSA enVision is:

- *Common Criteria Part 2 extended*, with security functional requirements based on functional components in Part 2 as well as the following;
    - EAN_ANL.1 Analyzer analysis,
    - EAN_COL.1 Event data collection,
    - EAN_RCT.1 Analyzer react,
    - EAN_RDR.1 Restricted data review;
- *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

- *Common Criteria EAL 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures

6 Security Policy

RSA enVision implements an administrator-configurable password strength policy. Details of this security policy can be found in section 7 of the Security Target.

7 Assumptions and Clarification of Scope

Consumers of RSA enVision 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 who are not careless, willfully negligent, or hostile, and will follow the instructions provided in the TOE documentation.

- The TOE can only be accessed by authorized users who have been assigned to manage it and the security of the information it contains.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The IT environment provides the TOE with appropriate physical security commensurate with the value of the IT assets protected by the TOE.

- The TOE environment will provide the physical protection to prevent unauthorized access.

- The IT Environment will provide reliable storage for event data, time stamps, authentication mechanisms and firewall rules to prevent access to the operating system of the TOE, and sufficient protection against disclosure of sensitive data transmitted between separate TOE components or between TOE components and trusted IT entities.

- The TOE environment will provide cryptographic functionality for collection protocols and web browsers when needed.

7.3 Clarification of Scope

The TOE provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks to violate system security, particularly from within the physical zone or domain of deployment. The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and communications security.

Consumers of the TOE should be aware of the following features and/or functionality that were not included as part of the evaluated configuration:

- The 60 Series appliances and their hardened version of Microsoft Windows Server 2003 Release 2 Enterprise Edition with Service Pack 2 operating system.
- National Vulnerability Database (NVD from Homeland Security) content updates
- RSA Vulnerability and Asset Management (VAM) tool content updates.
- Event Explorer, a desktop application for event tracing and incident management.
- External Network Attached Storage (NAS) or Direct Attached Storage (DAS) solutions.

8 Architectural Information

RSA enVision is a software-only TOE that is installed and deployed on general-purpose server hardware running a general-purpose operating system. The TOE consists of three components that can either be installed together all on one hardware appliance [ES deployment of 60 Series appliance], or each on their own appliance in distributed mode [LS deployment of 60 Series appliance].

Each deployment of the RSA enVision platform includes:

Application Server: The *Application Server* provides a Web User Interface (UI) for users to authenticate on prior to managing the TOE. Users can perform analysis, reporting, and various management functions. The *Alerter service* operates here and allows users to specify alerts based on events that need user attention when they occur. *Alerts* are actions the TOE can take automatically when a predefined set of events occur. Users can also specify *alerts* based on correlation rules. These rules identify sets of events and conditions to be met. The Web UI provides an interface for users to define alerts and correlation rules, apply rules to *alerts*, and define the actions for RSA enVision to take when an alert occurs.

Database Server: The *Database Server* receives requests for data from the *Application Server* and retrieves it from the storage device. It may return raw data or format the data as requested. Each enVision component generates audit messages and sends them to the *Database Server* which then formats and processes them in the same manner that it processes data from other event sources.

Local Collector: The *Local Collector* gathers data about devices on the network from logs and other forms of audit records. This data is obtained either through a Push collection, when the administrator has configured a device on the network to send event data to the TOE using supported push protocols, or using a Pull collection where the TOE is configured to actively retrieve data from a device on the network via supported pull protocols.

9 Evaluated Configuration

The TOE is software-only defined as:

- RSA enVision platform v4.0 SP 1 Build 0236

Two configurations were evaluated:

- The LS deployment comprises the Application Server, Database Server, and Local Collector each on a 60 Series LS appliance supplied by RSA.
- The ES deployment comprises the *ES component* (made up of the Application Server, Database Server, and Local Collector) installed on a single 60 Series ES appliance supplied by RSA.

Both configurations included the following 3rd party software and server operating system (OS) types:

- Microsoft Windows Server 2003 R2 Enterprise Edition SP2
- Sybase MySQL Anywhere v 9.0.2.3480

The 60 Series family of appliances comprise the following:

ES Series	LS Series
ES 560	LS A60
ES 1060	LS D60
ES 1260	LS L605
ES 2560	LS L610

ES 3060	LS R601
ES 5060	LS R602
ES 7560	

For more details on the two deployments, refer to section 1.4 of the ST.

10 Documentation

The RSA enVision documents provided to the consumer are as follows:

- RSA enVision Configuration Guide, v4.0, 2009;
- RSA enVision Hardware Guide 60 Series, v4.0, 2009;
- RSA enVision Migration Guide, v4.0, 2009;
- RSA enVision Universal Device Support Guide, v4.0, 2009
- RSA enVision Factory Re-Imaging and Typing, v4.0, 2009;
- RSA enVision Release Notes, v4.0, 2009;
- RSA enVision 4.0 Online Help (Web-based software);

11 Evaluation Analysis Activities

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

Development: The evaluators analyzed the RSA enVision 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 RSA enVision security architectural description and determined that the initialization process was 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 were correct.

Guidance Documents: The evaluators examined the RSA enVision preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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 were complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the RSA enVision configuration management system and associated documentation was performed. The evaluators found that the RSA enVision configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the RSA enVision design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

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

The evaluators reviewed the flaw remediation procedures used by RSA for RSA enVision during the site visit; the evaluators 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 RSA enVision. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators did not identify any potential vulnerabilities applicable to the RSA enVision in its operational environment.

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

12 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 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 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 and TOE design was complete.

The evaluators selected a sample of the developer test cases and repeated them during a site visit to the developer's QA facility using their lab resources. All test cases were easily duplicated with consistent results, thus gaining assurance in the developer testing method and practices.

12.2 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 EWA-Canada test goals:

- Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance;

- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator's TOE installation;

- Independent Evaluator Testing: The objective of this test goal is to exercise the TOE's claimed functionality through evaluator independent testing and to augment any areas that were not covered during the repeat of developer testing.

[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.

12.3 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:

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks.

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

12.4 Conduct of Testing

RSA enVision 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 Testing (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.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that RSA enVision behaves as specified in its ST and functional specification and TOE design.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The RSA enVision documentation set includes comprehensive installation, administration, deployment, development, user, and reference guides. The developer also provides a complete solution with on-site system engineer to help the customer integrate the TOE into a corporate network. 24/7 support is also an available option as well as training classes and material.

15 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
DAS	Direct Attached Storage
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NAS	Network Attached Storage
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
NVD	National Vulnerability Database (from Homeland Security)
QA	Quality Assurance
SFR	Security Functional Requirement
SIEM	Security Information Event Management
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
VAM	RSA Vulnerability and Asset Management tool

16 References

This section lists all documentation used as source material for this report:

- CCS Publication #4, Technical Oversight, Version 1.1, August 2005.
- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.
- Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

- RSA, The Security Division of EMC enVision® platform v4.0 SP 1 Security Target, 0.8, 11 December 2009

- Evaluation Technical Report for EAL 3+ Common Criteria Evaluation of RSA, The Security Division of EMC RSA enVision® platform v4.0 SP 1, Doc# 1625-000-D002, Version 1.3, 11 December 2009.