Certification Report

EAL 2+ Evaluation of RSA Archer eGRC Platform v5.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-173-CR
Version: 1.0
Date: 13 October 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 EWA-Canada located in Ottawa, 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 13 October 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).

This certification report makes reference to the following registered trademark:

- Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

TABLE OF CONTENTS

Executive Summary

RSA Archer eGRC Platform v5.0, from RSA, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

RSA Archer eGRC Platform v5.0 is an enterprise Governance, Risk and Compliance (eGRC) software solution that provides a platform for building applications to solve specific enterprise business needs and manages user interaction with the applications. Users are not permitted to read application code or data, write or modify application code or data, or execute specific application tasks unless they have been properly authorized to do so. User access is controlled at the system, application, record and field levels.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 30 September 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 RSA Archer eGRC Platform v5.0, 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.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that RSA Archer eGRC Platform v5.0 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 RSA Archer eGRC Platform v5.0, from RSA.

2 TOE Description

RSA Archer eGRC Platform v5.0 is an enterprise Governance, Risk and Compliance (eGRC) software solution that provides a platform for building applications to solve specific enterprise business needs and manages user interaction with the applications. Users are not permitted to read application code or data, write or modify application code or data, or execute specific application tasks unless they have been properly authorized to do so. User access is controlled at the system, application, record and field levels.

A description of the RSA Archer eGRC Platform v5.0 architecture is found in Section 1.4 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for RSA Archer eGRC Platform v5.0 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: RSA, The Security Division of EMC RSA Archer eGRC Platform v5.0 Security Target
Version: 0.6
Date: 20 September 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.*

The RSA Archer eGRC Platform v5.0 is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
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*, with all security the assurance requirements in the EAL 2 package as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

The RSA Archer eGRC Platform v5.0 implements a role-based access control policy to control administrator access to the TOE, as well as a discretionary access control policy to control user access to the applications executed by the TOE and the information stored in the TOE. Further details on these policies can be found in Sections 6.2.2 and 6.2.4 of the ST.

In addition, the RSA Archer eGRC Platform v5.0 implements policies pertaining to Security Audit, Identification and Authentication, Security Management, and TOE Access. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of RSA Archer eGRC Platform v5.0 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:

a. Competent, non-hostile, and appropriately trained individuals manage the TOE.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

a. The TOE is installed on appropriate hardware and operating system software.

b. The TOE is located in a protected facility.

c. The IT environment provides the secure protocols necessary to protect the communication path between the TOE, end users, and the remote authentication server.

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

7.3 Clarification of Scope

The RSA Archer eGRC Platform v5.0 is not intended to be placed or operated in a hostile environment, and should be protected by other products specifically designed to address sophisticated threats.

8 Evaluated Configuration

The evaluated configuration for RSA Archer eGRC Platform v5.0 comprises the 32 and 64-bit RSA Archer eGRC Platform v5.0.2.1130 software running on:

a. Microsoft Windows 2003 Server with IIS Version 6.0 and Microsoft SQL Server 2005; and
b. Microsoft Windows 2008 Server with IIS Version 7.0 and Microsoft SQL Server 2008.

The evaluated configuration requires the Internet Explorer 7 web browser and Microsoft Windows Active Directory.

The publication entitled *RSA Archer eGRC v5.0 Guidance Documentation Supplement* describes the procedures necessary to install and operate RSA Archer eGRC Platform v5.0 in its evaluated configuration.

9 Documentation

The RSA documents provided to the consumer are as follows:

a. RSA Archer eGRC Platform Administrator Guide Online Help File v5.0;
b. RSA Archer eGRC Platform User Guide Online Help File v5.0;
c. RSA Archer eGRC Platform Control Panel Online Help File v5.0;
d. RSA Archer eGRC Platform Installation Guide v5.0;
e. RSA Archer eGRC Platform Release Notes v5.0;
f. RSA Archer eGRC Guidance Documentation Supplement v0.3; and
g. RSA Archer eGRC Web Services API3 Guide v5.0.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of RSA Archer eGRC Platform v5.0, including the following areas:

Development: The evaluators analyzed the RSA Archer eGRC Platform v5.0 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 Archer eGRC Platform v5.0 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 RSA Archer eGRC Platform v5.0 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 RSA Archer eGRC Platform v5.0 configuration management system and associated documentation was performed. The evaluators found that the RSA Archer eGRC Platform v5.0 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 RSA Archer eGRC Platform v5.0 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by RSA for RSA Archer eGRC Platform v5.0 . 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 RSA Archer eGRC Platform v5.0. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify RSA Archer eGRC Platform v5.0 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the RSA Archer eGRC Platform v5.0 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].

[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.

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.

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 on the evaluator's TOE installation;

b. 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;

c. Account Management and Secure Auditing: The objective of this test goal is to exercise the TOE's claimed user account management and audit functionality;

d. Management of Security Parameters: The objective of this test goal is to verify that password composition and login attempt rules are enforced; and

e. User Data Protection: The objective of this test goal is to verify that user data is protected from unauthorized access using groups and roles.

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 Scanning: The objective of this test goal is to use automated vulnerability scanning tools to determine which services are listening or available. An attempt to obtain a signature of the host operating system is also performed; and

b. Misuse by TOE user: The objective of this test goal is to verify that an operator of the TOE, while not intentionally malicious, is prevented from disrupting the proper operation of the TOE through invalid use of processes or configuration parameters.

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

11.4 Conduct of Testing

RSA Archer eGRC Platform v5.0 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 RSA Archer eGRC Platform v5.0 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

Documentation for the RSA Archer eGRC Platform v5.0 includes comprehensive installation and development guides as well as online help.

14 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
eGRC	Enterprise Governance Risk Compliance
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
SFP	Security Function Policy

Acronym/Abbreviation/ Initialization	Description
SFRs	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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. RSA, The Security Division of EMC RSA Archer eGRC Platform v5.0 Security Target, Revision No. 0.6, 20 September 2011.

e. Evaluation Technical Report (ETR) RSA Archer eGRC Platform v5.0, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-173, Document No. 1671-000-D002, Version 1.2, 23 September 2011.