Certification Report

BMC Remedy Action Request System with Premium Encryption Security v8.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-253-CR
Version: 1.0
Date: 30 March 2015
Pagination: i to iii, 1 to 10

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 30 March 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).

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

- Linux is a registered trademark of Linus Torvalds Inc.;
- BMC and BMC Software are registered trademarks of BMC Software, Inc.;
- IBM and DB2 are registered trademarks of International Business Machines Corporation;
- Microsoft, Windows and Windows Server are registered trademarks of Microsoft Corporation;
- BSAFE is a registered trademark of RSA Security;
- Oracle, Solaris and Java are registered trademarks of Oracle; and
- UNIX is a registered trademark of The Open Group.

TABLE OF CONTENTS

Executive Summary

BMC Remedy Action Request System with Premium Encryption Security v8.1 (hereafter referred to as BMC Remedy Action Request System), from BMC Software, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that BMC Remedy Action Request System meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

BMC Remedy Action Request System is a development and runtime platform used to build applications that automate business processes. It also gives customers the ability to design and customize workflow-based applications to automate business processes. Using BMC Remedy Action Request System, nonprogrammers can build business workflow applications and deploy them simultaneously in web, Windows, UNIX®, and Linux® environments. One of the most common uses of BMC Remedy Action Request System is to automate internal service desks.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 30 March 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 BMC Remedy Action Request System, 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 BMC Remedy Action Request System 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).

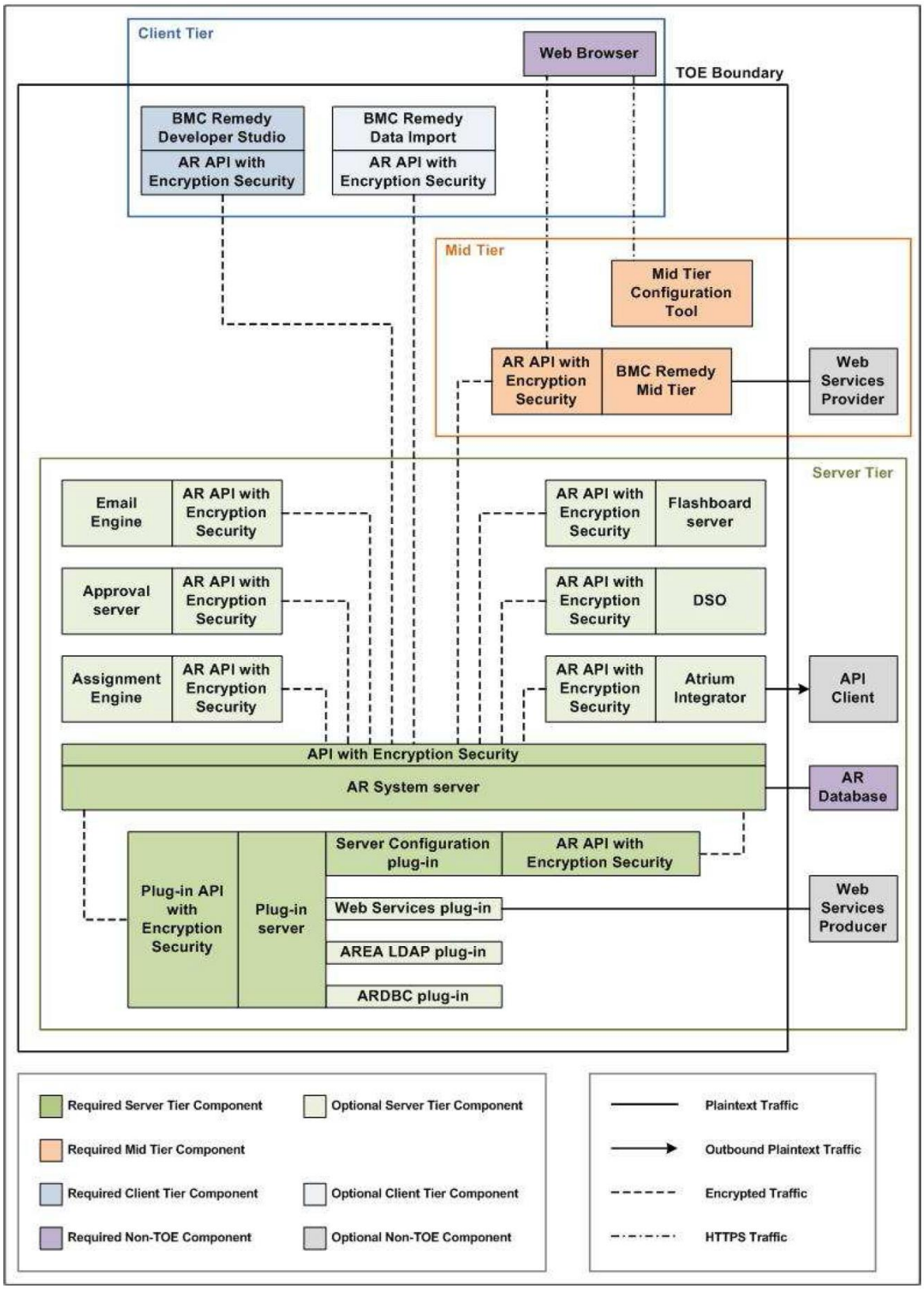
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is BMC Remedy Action Request System with Premium Encryption Security v8.1 (hereafter referred to as BMC Remedy Action Request System), from BMC Software, Inc..

2 TOE Description

BMC Remedy Action Request System is a development and runtime platform used to build applications that automate business processes. It also gives customers the ability to design and customize workflow-based applications to automate business processes. Using BMC Remedy Action Request System, nonprogrammers can build business workflow applications and deploy them simultaneously in web, Windows, UNIX®, and Linux® environments. One of the most common uses of BMC Remedy Action Request System is to automate internal service desks.

A diagram of the BMC Remedy Action Request System architecture is as follows:


Client Tier
Web Browser
TOE Boundary
BMC Remedy Developer Studio
AR API with Encryption Security
BMC Remedy Data Import
AR API with Encryption Security
Mid Tier
Mid Tier Configuration Tool
AR API with Encryption Security
BMC Remedy Mid Tier
Web Services Provider
Server Tier
Email Engine
AR API with Encryption Security
AR API with Encryption Security
Flashboard server
Approval server
AR API with Encryption Security
AR API with Encryption Security
DSO
Assignment Engine
AR API with Encryption Security
AR API with Encryption Security
Atrium Integrator
API Client
API with Encryption Security
AR System server
AR Database
Plug-in API with Encryption Security
Plug-in server
Server Configuration plug-in
AR API with Encryption Security
Web Services plug-in
Web Services Producer
AREA LDAP plug-in
ARDBC plug-in
Required Server Tier Component
Optional Server Tier Component
Required Mid Tier Component
Required Client Tier Component
Optional Client Tier Component
Required Non-TOE Component
Optional Non-TOE Component
Plaintext Traffic
Outbound Plaintext Traffic
Encrypted Traffic
HTTPS Traffic

3 Security Policy

BMC Remedy Action Request System implements a role-based access control policy to control administrative access to the system. In addition, BMC Remedy Action Request System implements policies pertaining to the following security functional classes:

Security Audit;

Cryptographic Support;

User Data Protection;

Identification and Authentication;

Security Management; and

Protection of the TSF (TOE Security Function).

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

Cryptographic Module	**Certificate**
OpenSSL FIPS Object Module	*1051*
Network Security Services (NSS) version 3.11.4	*815*

4 Security Target

The ST associated with this Certification Report is identified below:

BMC Remedy Action Request System with Premium Encryption Security v8.1 Security Target, version 0.07, January 24, 2014.

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.*

BMC Remedy Action Request System 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:*

- FPT_APP_EXP – Application Server Authentication.

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 BMC Remedy Action Request System 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 software has been installed and set up in accordance with the delivery and installation procedures;
- One or more authorised administrators will be assigned to install, configure and manage the TOE and the security of the information it contains; and
- Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The operational environment will provide a reliable time source;
- The Operating System will provide discretionary access control (DAC);
- Any system with which the TOE communicates is assumed to be under the same security policy constraints as the TOE;
- The processing resources of the TOE will be located within facilities providing controlled access;
- The TOE operational environment will provide the ability to configure SSL communications where appropriate; and
- All supporting operational environment components have had all current security patches, if applicable, applied and are secured;

7 Evaluated Configuration

The evaluated configuration for BMC Remedy Action Request System with Premium Encryption Security v8.1 comprises the following components:

- BMC Remedy Developer Studio version 8.1.00; and
- BMC Remedy Data Import version 8.1.00;

As the Client Tier on a Windows 7 operating system.

- BMC Remedy Mid-Tier and Configuration Tool version 8.1.00;

As the Mid Tier on either a Windows Server 2008 R2 SP1 or a Solaris 10 update 11 operating system.

- BMC Remedy Action Request System Server version 8.1.00;
- Server Configuration plug-in version 8.1.00;
- Web Services plug-in version 8.1.00;

- BMC Atrium Integrator version 8.1.00;
- BMC Remedy Premium Encryption version 8.1.00;
- BMC Remedy Email Engine version 8.1.00;
- BMC Remedy Approval Server version 8.1.00;
- BMC Remedy Flashboards Server version 8.1.00;
- BMC Remedy Distributed Server Option version 8.1.00;
- AREA LDAP plug-in version 8.1.00;
- ARDBC plug-in version 8.1.00; and
- BMC Remedy Assignment Engine version 8.1.00.

As the Server Tier on either a Windows Server 2008 R2 SP1 or a Solaris 10 update 11 operating system.

The publications entitled BMC® Remedy® Action Request System® with Premium Encryption Security v8.1 Guidance Supplement, 0.01, 14 February 2014 and BMC Remedy Action Request System Version 8.1.00 Online Documentation, Version 8.1.00, 2013 describe the procedures necessary to install and operate BMC Remedy Action Request System in its evaluated configuration.

8 Documentation

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

a. BMC® Remedy® Action Request System® with Premium Encryption Security v8.1 Guidance Supplement, 0.01, 14 February 2014; and
b. BMC Remedy Action Request System Version 8.1.00 Online Documentation, Version 8.1.00, 2013.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of BMC Remedy Action Request System, including the following areas:

Development: The evaluators analyzed the BMC Remedy Action Request System 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 BMC Remedy Action Request System 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 BMC Remedy Action Request System 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 BMC Remedy Action Request System configuration management system and associated documentation was performed. The evaluators found that the BMC Remedy Action Request System 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 BMC Remedy Action Request System during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the BMC Remedy Action Request System. 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;

[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.

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 ST;

c. Logins:

    a. As Sub-Administrator: The objective of this test goal is to show that a Sub-Administrator may login but have minimal permissions;

    b. As Administrator: The objective of this test goal is to show that an Administrator may login and be able to manage the TOE;

d. Associate Security Values: The objective of this test goal is to demonstrate that the BMC Remedy Action Request System associates the values of the security attributes user name and password with the session.

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.

b. Search Public Domain information sources for vulnerabilities for the TOE, paying close attention to the Heartbleed vulnerability, the Poodle vulnerability and the Shellshock vulnerability; and

c. Information Leakage Verification: The objective of this test goal is to determine if there is any leakage during start-up, shutdown, login, and other scenarios where there is communication between parts of the TOE.

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

10.4 Conduct of Testing

BMC Remedy Action Request System 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 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.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that BMC Remedy Action Request System 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 Evaluator Comments, Observations and Recommendations

The evaluator recommends that the users read the ST and make sure all the assumptions made regarding the environment are true in the intended environment of the TOE. The potential users of the TOE should also follow all the instructions and recommendations provided in the documents during installation and configuration of the TOE.

Given the extensive set of user guidance, the evaluator strongly recommends users of the TOE consult the Guidance Supplement for references on relevant user guidance in order to configure the TOE in its evaluated configuration.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
ARDBC	Action Remedy Database Connectivity
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LDAP	Lightweight Directory Access Control
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

14 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. BMC Remedy Action Request System with Premium Encryption Security v8.1 Security Target, version 0.07, January 24, 2014

e. Evaluation Technical Report for BMC Remedy Action Request System with Premium Encryption Security v8.1, version 1.0, 30 March 2015.