National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

BMC Remedy Action Request System 7.5.00 Patch 007

Report Number:	CCEVS-VR-VID10383-2011
Dated:	31 October 2011
Version:	1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin
Nicole Carlson

The Aerospace Corporation
El Segundo, CA

Common Criteria Testing Laboratory

James L. Arnold, Jr.
M. Eve Pierre
Quang Trinh

Science Applications International Corporation
Columbia, MD

Table of Contents

1 Executive Summary

This Validation Report (VR) documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the BMC Remedy Action Request (AR) System 7.5.00 Patch 007 product with BMC Remedy AR System Encryption Security 7.5.00. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the United States of America (USA) government, and no warranty is either expressed or implied. The TOE is identified in section 2 of this report.

The evaluation was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA and was completed in October 2011. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of Evaluation Assurance Level (EAL) 4.

The BMC Remedy Action Request System 7.5.00 Patch 007 with BMC Remedy Encryption Security 7.5.00 Target of Evaluation (TOE) provides a consolidated Service Process Management platform for automating and managing Service Management business processes. With its request-centric, workflow-based architecture, AR System is optimized for efficiencies in Service Management business process delivery.

The TOE has been evaluated at a NIAP-approved CCTL 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 evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the CCTL in the Evaluation Technical Report (ETR) are consistent with the evidence provided.

This VR applies only to the specific version of the TOE as evaluated. The TOE, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the BMC Remedy Action Request System 7.5.00 Security Target (ST), Version 1.10, October 2011.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and versions of the ETR. Also, at some discrete points during the evaluation, Validators formed a Validation Oversight Review (VOR) panel in order to review the ST and other evaluation evidence along with the corresponding evaluation findings in detail. The validation team found that the evaluation showed that the product satisfies all of the security functional requirements (SFRs) and security assurance requirements (SARs) stated in the ST. Therefore the validation team concludes that the CCTL’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the CCTL in the ETR are consistent with the evidence produced.

The technical information included in this VR was obtained from the Final ETR for BMC Remedy Action Request System 7.5.00 parts 1 and 2 and the associated test report produced by SAIC. Part 1 is intended for the general public; part 2 is BMC and SAIC proprietary.

1.1 Evaluation Details

Item	Identifier
Evaluated Product:	BMC Remedy Action Request System 7.5.00 Patch 007, with BMC Remedy Premium Encryption Security 7.5.00 or with BMC Remedy Performance Encryption Security 7.5.00 English version
Evaluation Class:	Evaluation Assurance Level (EAL) 4
Conformance Result:	Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant
Developer and Sponsor:	BMC Software, Inc. 91 E. Tasman Drive San Jose, CA 95134
Validation Scheme:	National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS)
Validation Personnel:	The Aerospace Corporation • Daniel Faigin • Nicole Carlson
Common Criteria (CC) Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, September 2009
Interpretations:	None
Common Evaluation Method (CEM) Identification:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 3, September 2009
Protection Profile (PP):	None
CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel:	Science Application International Corporation • James L. Arnold, Jr. • M. Eve Pierre • Quang Trinh

Item	Identifier
Description:	The TOE is the BMC Remedy Action Request System 7.5.00[1], which provides a consolidated Service Process Management platform for automating and managing Service Management business processes. Note: The evaluation did not cover the correct operation of the service process management functions or process flow capabilities provided by BMC Remedy applications developed and run on the BMC Remedy AR System platform. Rather the evaluation focused on the security-related functions used to manage, protect, and monitor those core product capabilities.
Disclaimer:	The information contained in this VR is not an endorsement of the BMC Remedy Action Request System 7.5.00 Patch 007 with BMC Remedy Encryption Security 7.5.00 by any agency of the U.S. Government and no warranty of BMC Remedy Action Request System is either expressed or implied.

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- A user might be able to repudiate their use of privileged functions protected by the TOE Security Functions (TSF).
- An unauthorized user or subject might gain access to user data protected by the TOE or TSF data to view, modify, or delete that data, or execute system applications or modify system applications in order to disrupt, or otherwise hinder, business operations.
- Human users of the TOE might attempt to view, modify, or delete TOE objects, or execute or modify applications for which they do not have the prescribed authority, as specified by local policy, in order to disrupt, or otherwise hinder, business operations.
- Administrators of the TOE might not have utilities sufficient to effectively manage the security features.

1.4 Organizational Security Policies

The ST does not identify any organizational security policies that the TOE and its operational environment are intended to fulfill.

[1] Patch 007, English version

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with the national Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List (VPL).

The evaluated product, or TOE, is identified below:

Security Target: BMC Remedy Action Request System 7.5.00 Security Target, Version 1.10, October 2011

TOE Identification: BMC Remedy Action Request System 7.5.00 Patch 007, with BMC Remedy Premium Encryption Security 7.5.00 or with BMC Remedy Performance Encryption Security 7.5.00 (English version) including the following components:

- BMC Remedy Action Request System Server 7.5.00 (patch 007)
- BMC Remedy Approval Server 7.5.00 (patch 007)
- BMC Remedy Email Engine 7.5.00 (patch 007)
- BMC Remedy Flashboards Server 7.5.00 (patch 007)
- Action Request System External Authentication LDAP plug-in 7.5.00 (patch 007)
- Action Request System Database Connectivity plug-in 7.5.00 (patch 007)
- BMC Remedy Mid Tier 7.5.00 (patch 007)
- BMC Remedy Developer Studio 7.5.00 (patch 007)
- BMC Remedy User 7.5.00 (patch 007)
- BMC Remedy Data Import 7.5.00 (patch 007)
- BMC Remedy Alert 7.5.00 (patch 007)
- BMC Remedy Mid Tier Configuration Tool 7.5.00 (patch 007)
- BMC Remedy Distributed Server Option 7.5.00 (patch 007)
- BMC Remedy Assignment Engine 7.5.00 (patch 007)

Operating Platform: Operating System

- Microsoft Windows Server 2003 (32- or 64-bit) or higher
- Sun Solaris 9 or higher

Database

- Oracle 10G (R2) or higher
- Microsoft SQL Server 2005 or higher

Web Server

- Microsoft Internet Information Server (IIS) 6 or higher
- Tomcat 5.5.28 or higher

Servlet Engine

- Tomcat 5.5.28 or higher
- Java SDK/JRE 1.5.0 and 1.6.0_06 or higher

Java SDK/JRE

- Java SDK/JRE 1.5.0 and 1.6.0_06 or higher

E-Mail

- Any mail server using SMTP or MAPI standard protocols, such as Microsoft Exchange (Windows Server 2003)

LDAP Directory Service

- Any directory service using the LDAP standard protocol such as Microsoft Active Directory (Windows Server 2003)

Web Browser

- Microsoft Internet Explorer 6 or higher

3 Security Policy

The BMC Remedy Action Request System 7.5.00 Patch 007 TOE enforces the following security policies as described in the ST.

- User Data Protection
- Identification and Authentication
- Security Audit
- Security Management
- Encryption

Note: Much of the description here has been drawn from the BMC Remedy Action Request System 7.5.00 ST and Final ETR. The ST, in particular, should be consulted for more description of these and other security functions of the TOE.

3.1 User Data Protection

Access to TOE data is controlled by the use of access control groups. A user's inclusion within a group, or groups, is established by the administrator in accordance with the locally specified access control policy (GRP_ACC_CTRL). AR System allows the administrator to set group-based permissions on various types of AR System controlled objects. This allows the administrator to control access at multiple levels, including applications and the components of applications, and data at the level of forms (tables), requests (rows), and fields (columns). Groups further determine the type of operational access that group members have at each level, including view, modify, create, delete, execute, and no access. The AR System Server enforces access control at each level of access.

AR System roles allow an administrator designing an application to assign access control to application objects by AR System role, and each role is mapped to an access control group. In this way, when the application is distributed to local systems, access control by groups is maintained across a distributed network having differing group names that support similar roles. In this document, the term AR System roles is used to refer to this method of assigning permissions in AR System, while the term "roles" refers to the CC concept of a defined relationship governing the allowed interactions between a user and the TOE.

3.2 Identification and Authentication

The TOE identifies users by the user name, which is stored in BMC Remedy Action Request System. By default, users who access BMC Remedy based solutions through BMC Remedy User or a web browser are prompted for a user name and password by AR System, and must be identified and authenticated before they can access the system. After identification and authentication, the user name is then used as part of every AR System Server request, since no action can be taken unless a valid user name is associated with it.

AR System prompts the user for a user name and password.

- If AR System is not configured to use external authentication, the AR System Server searches for the user name in the User form. If a match is found, the AR System Server compares the password entered by the user with that stored in the User form. If the user name and password both match, the user is authenticated.

- If AR System is configured for external authentication, the user name and password entered are passed to the operating system (Windows or UNIX) or to an LDAP server in the operational environment. The operating system or LDAP server matches the user name, and authenticates the password, before the user can access the AR System. In this case, the user name assigned in AR System must match the user name in the external authenticating environment exactly. Configuring AR System to use external authentication is controlled from the AR System Administration: Server Information form, accessed through BMC Remedy User or a browser.

In the evaluated configuration, the administrator must configure AR System to prevent anonymous access. There are two parts to this configuration. The administrator must replace the default administrator account and password with an administrator-designated administrator account and password. The administrator must configure AR System to prevent access by guest users.

3.3 Security Audit

The TOE provides the ability to audit all interaction between clients and the AR System Server, and between the AR System Server and the database, including API calls between clients and server, SQL requests from the AR System Server to the database server, user authentication attempts, and several other log types. The administrator can also configure the BMC Remedy Encryption Security products to report audit data to a log file. The TOE relies on the operational environment to store and protect the audit data. It also relies on the TOE environment to provide an appropriate time stamp for use in the audit records. The TOE can be configured to store the audit records in a form, in which case, the audit records are reviewed using the BMC Client interfaces; or they can be stored in files on the OS directory. When the audit records are stored in files on the OS, the audit records are reviewed using the log viewer provided with the TOE or with a text editor provided by the TOE environment.

3.4 Security Management

The TOE provides administrators with interfaces to manage security policy and its implementation in BMC Remedy User, the AR System Administration Console, BMC Remedy Developer Studio, and the BMC Remedy Mid Tier Configuration Tool. These clients allow the administrator to manage server objects and system configuration settings, and to control access to AR System by human users, BMC Remedy based applications, and other external clients.

All user access definition and management is performed through forms that are accessible to Authorized administrators in BMC Remedy User or through a browser. Policy management and implementation are controlled through the use of access control groups and security role definitions and privileges. Access control groups are the basis by which all user access is granted. Access control in AR System is additive. Each user starts out with no access to AR System controlled objects, and Authorized administrators or Authorized subadministrators add permissions as needed. Authorized administrators can set default permissions and specific permissions on objects in AR System, and Authorized subadministrators can set specific permissions to objects where assigned.

Roles, including security roles, are specified in the AR System by membership in groups. The AR System reserves eight group IDs for special group definitions with associated access privileges, including the groups Administrator and Subadministrator. Members of the Administrator group have the security role Authorized administrator. Members of the Subadministrator group have the security role Authorized subadministrator.

Configuration of application servers, including application server passwords, is controlled by Authorized administrators using the AR System Administration: Server Information form and other forms accessible to the administrator through BMC Remedy User or a browser. Many settings managed in the AR System Administration: Server Information forms are stored in the server configuration file (ar.cfg on Windows or ar.conf on UNIX). The administrator must protect this and other configuration files from tampering by setting the appropriate directory permissions and file settings. In addition to the file protections assumed to be provided by the operational environment, application service passwords stored in configuration files are obfuscated using a proprietary implementation of DES.

3.5 Encryption

The TOE includes BMC Remedy Encryption (either BMC Remedy Encryption Premium Security or BMC Remedy Encryption Performance Security.) They are sold and installed separately from AR System and the evaluated configuration of the TOE must include one of these products. The customer determines which level to purchase based on the level of encryption required. Both products can be configured use a Federal Information Processing Standards (FIPS)-certified encryption algorithm. While the BMC Remedy Encryption Security products have not been independently FIPS-validated, these products include both the OpenSSL FIPS Object Module, version 1.2 (FIPS 140-2 certificate number 1051) and the RSA BSAFE Crypto-J JCE Provider Module, version 3.5.2 (FIPS 140-2 certificate number 714). All components that access the C Application Programming Interface (API) use the FIPS-certified OpenSSL module (FIPS 140-2 certificate number 1473). The FIPS-certified RSA BSAFE module (FIPS 140-2 certificate number 1359) is used for the Java API, which includes the mid-tier component. When installed and configured, these products provide encryption of network communications between AR System components. These products are installed and operate on the server tier, the mid tier, and the client tier. The BMC Remedy Encryption Security libraries are installed on all computers running any component of the TOE. The library files and log files are protected by operating system access control rights on each computer where the product is installed.

4 Assumptions

The ST, section 3.1.1 “Environmental assumptions”, identifies the following assumptions required to ensure the security of the TOE:

- Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. This includes the network. (The network operates under the same constraints and resides within a single management domain).
- The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical access.
- The underlying platform(s) upon which the TOE executes and all other components in the operational environment [including the operating system, database, email server, and Lightweight Directory Access Protocol (LDAP) server] will provide reliable functionality including correct hardware operation and functionality, and correct platform software operation.
- The TOE software has been delivered, installed, and set up in accordance with documented delivery and installation/setup procedures and the evaluated configuration.
- There will be one or more competent Authorized Administrators assigned to manage the TOE and the security functions it performs. Procedures will exist for granting Authorized Administrators access to the TSF.
- An Authorized Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation.
- The host platform operating system of the TOE environment will provide discretionary access control (DAC) to protect TOE executables and TOE data.
- All supporting operational environment components (such as the operating system, database, web browser, web server, email server, and LDAP server) have had all current security patches (if applicable) applied, and the Authorized Administrator has configured the inherent component security mechanisms to their most restrictive settings that will still permit TOE functionality and interoperability. Any such patch does not interfere with the correct functioning of AR System Server’s interfaces to the supporting operational environment components.
- The TOE environment may provide authentication mechanisms, as described in the Security Target, section 6.1.4, Table 11: Types of external authentication, and these mechanisms will function correctly and accurately.
- The operational environment will provide reliable system time.
- The TOE operational environment will provide the ability to configure SSL communications where appropriate.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 4 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 4 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that might be exploitable by an attacker with moderate or higher attack potential. The definition of attack potential is rather complex and the Common Evaluation Methodology (CEM), annex B.4, should be consulted for more information in this context.
4. The evaluation did not analyze, explore or test the correct operation of the business functions implemented by the TOE. Rather, the evaluation focused specifically on the security functions surrounding the use of those functions.
5. The TOE relies on the environment in which it operates for the following security and other functionality:
    - Protect the TOE's stored executable image and its execution environment.
    - Protect the TOE's stored audit and other data and provide a means to review audit data stored in text files.
    - Provide a reliable time stamp for use in audit records.
    - Protect communication between TOE components and client browsers and LDAP servers to protect sensitive data (e.g., passwords).
    - Provide external authentication services via LDAP.
6. The following product capabilities described in the guidance documentation were not included within the scope of the evaluation and no claims are made regarding them:
    - Only outgoing Email Engine functionality, for the purpose of sending notifications, is included in the evaluated configuration. Submission and modification of requests through the Email Engine is not included in the evaluated configuration.
    - Additional functionality is provided by the following applications and they may be used in the operational environment of the TOE and accessed by the TOE clients as application objects, when so configured, subject to TOE access control policies. However, as applications that run on the AR System platform they are not part of the TOE and are not included in the evaluated configuration.
        - BMC Atrium Configuration Management Database
        - BMC Atrium Integration Engine
        - BMC Remedy Asset Management
        - BMC Remedy Change Management
        - BMC Remedy Service Desk (includes BMC Remedy Incident Management and BMC Remedy Problem Management)
        - BMC Service Level Management
        - BMC Service Request Management

5 Architectural Information

The BMC Remedy Action Request System 7.5.00 is a development and runtime platform used to build applications that automate business processes. It also gives customers with or without programming experience the ability to design and customize workflow-based applications to automate business processes. Using AR 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 7.5.00 is to automate internal service desks.

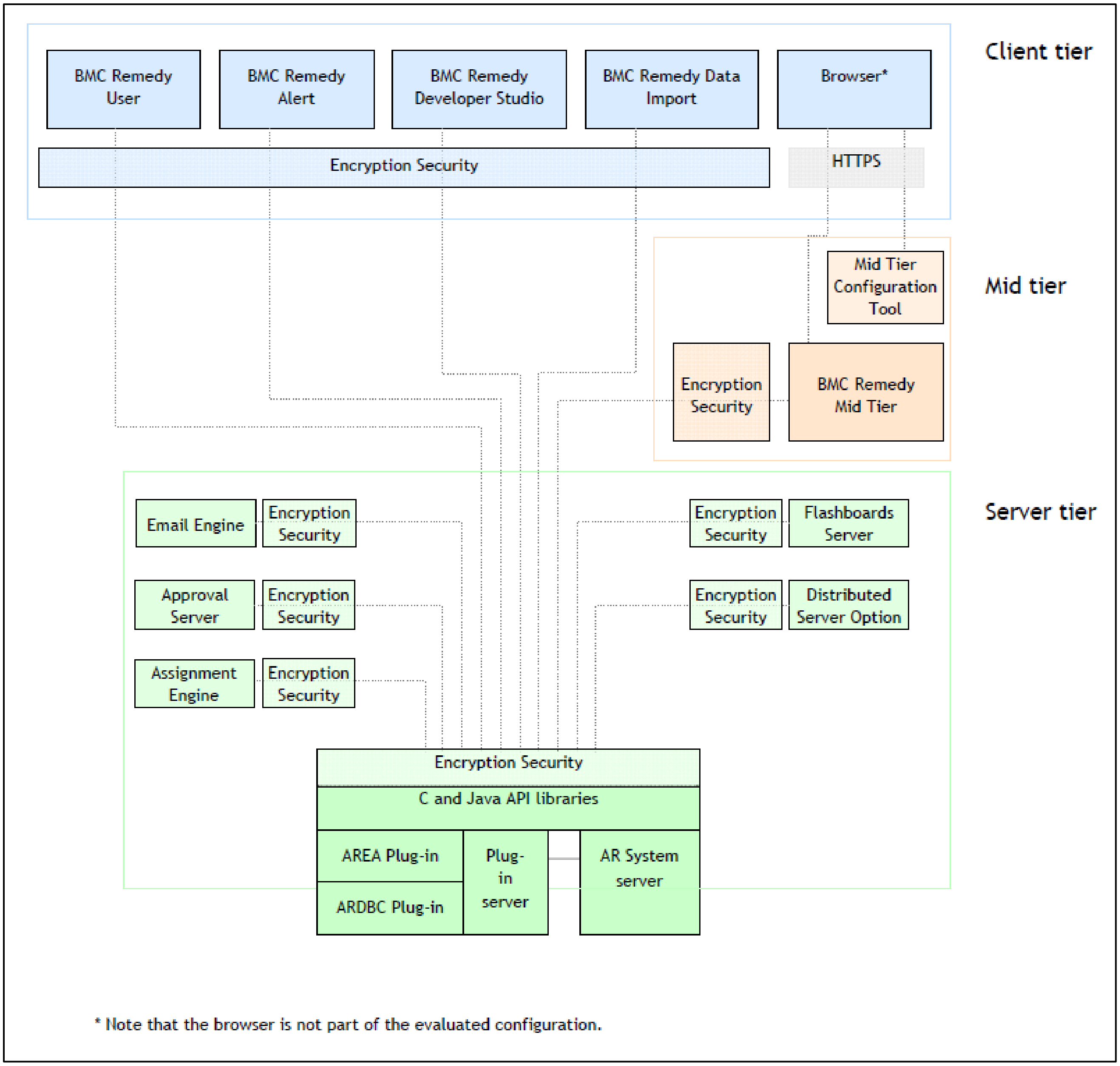
The following list identifies the BMC Remedy Action Request System 7.5.00 Patch 007 components and versions included in the evaluated configuration:

- BMC Remedy Action Request System Server 7.5.00 (patch 007)
- BMC Remedy Approval Server 7.5.00 (patch 007)
- BMC Remedy Email Engine 7.5.00 (patch 007)
- BMC Remedy Flashboards Server 7.5.00 (patch 007)
- Action Request System External Authentication LDAP plug-in 7.5.00 (patch 007)
- Action Request System Database Connectivity plug-in 7.5.00 (patch 007)
- BMC Remedy Mid Tier 7.5.00 (patch 007)
- BMC Remedy Developer Studio 7.5.00 (patch 007)
- BMC Remedy User 7.5.00 (patch 007)
- BMC Remedy Data Import 7.5.00 (patch 007)
- BMC Remedy Alert 7.5.00 (patch 007)
- BMC Remedy Mid Tier Configuration Tool 7.5.00 (patch 007)
- BMC Remedy Distributed Server Option 7.5.00 (patch 007)
- BMC Remedy Assignment Engine 7.5.00 (patch 007)

The following list identifies the BMC Remedy Encryption Security 7.5.00 (no patch) components and versions included in the evaluated configuration:

- BMC Remedy Encryption Performance Security 7.5.00
- BMC Remedy Encryption Premium Security 7.5.00

Figure 1 below illustrates the TOE as it can be deployed in a customer environment. Note that while the figure depicts three tiers, the TOE can be deployed as either two or three tiers where either the mid or client tier could be absent. Further note that the independent evaluation testing did not cover the situation where the AR System is deployed only with a mid-tier since that is a generally unrealistic deployment.



* Note that the browser is not part of the evaluated configuration.

Figure 1. BMC Remedy Actions Request System 7.5.00

5.1 Physical Boundaries

As indicated above, the TOE is a series of components organized into tiers. The components listed in the "TOE component" column are included in the TOE.

Note: Note that either Premium Encryption or Performance Encryption is required, not both.

TOE component	Dependencies	Optional Y/N	Version	Underlying environment
BMC Remedy Action Request System Server	o A database	N	7.5.00 patch 007	o Microsoft Windows Server 2003 (32- or 64-bit) or higher o Sun™ Solaris™ 9 or higher
BMC Remedy Premium Encryption	o AR System Server	N	7.5.00	o Microsoft Windows Server 2003 (32- or 64-bit) or higher o Sun Solaris 9 or higher
BMC Remedy Performance Encryption	o AR System Server	N	7.5.00	o Microsoft Windows Server 2003 (32- or 64-bit) or higher o Sun Solaris 9 or higher
BMC Remedy Mid Tier and Configuration Tool	o AR System Server o Web server o Servlet Engine o Java Software Developers' Kit (SDK)/ Java Runtime Environment (JRE) o Browser	Y	7.5.00 patch 007	o Microsoft Windows Server 2003 (32- or 64-bit) or higher o Sun Solaris 10 or higher
BMC Remedy User	o AR System Server	o Y if the mid tier is installed. o N if the mid tier is not installed.	7.5.00 patch 007	o Windows XP, 32-bit or higher
BMC Remedy Alert	o AR System Server	Y	7.5.00 patch 007	o Windows XP, 32-bit or higher

TOE component	Dependencies	Optional Y/N	Version	Underlying environment
BMC Remedy Developer Studio	o AR System Server o Java SDK/JRE	N	7.5.00 patch 007	o Windows XP, 32-bit or higher
BMC Remedy Data Import	o AR System Server o Java SDK/JRE	N	7.5.00 patch 007	o Windows XP, 32-bit or higher
BMC Remedy Email Engine	o AR System Server o Java SDK/JRE o An email exchange server	Y	7.5.00 patch 007	o Same as AR System Server platform
BMC Remedy Approval Server	o AR System Server	Y	7.5.00 patch 007	o Same as AR System Server platform
BMC Remedy Flashboards	o BMC Remedy Mid Tier o AR System Server	Y	7.5.00 patch 007	o Same as AR System Server platform
BMC Remedy Distributed Server Option	o AR System Server	Y	7.5.00 patch 007	o Same as AR System Server platform
AREA LDAP plug-in	o AR System Server o LDAP directory service (optional)	Y	7.5.00 patch 007	o Same as AR System Server platform
ARDBC plug-in	o AR System Server	Y	7.5.00 patch 007	o Same as AR System Server platform
BMC Remedy Assignment Engine	o AR System Server	Y	7.5.00 patch 007	o Same as AR System Server platform

The following additional components are supported in the operational environment:

Environment component	Dependencies	Optional Y/N	Version	Underlying environment
Operating system	None	N	o Microsoft Windows Server 2003 (32- or 64-bit) or higher o Sun Solaris 9 or higher	As appropriate

Environment component	Dependencies	Optional Y/N	Version	Underlying environment
Database	o Operating system o ARSystem server	N	o Oracle 10G (R2) or higher o Microsoft SQL Server 2005 or higher	As appropriate
Web server	o Operating system	o N if the mid tier is installed. o N/A if the mid tier is not installed.	o Microsoft Internet Information Server (IIS) 6 or higher o Tomcat 5.5.28 or higher	As appropriate
Servlet Engine	o Web Server o Java SDK/JRE	o N if the mid tier is installed. o N/A if the mid tier is not installed.	o Tomcat 5.5.28 or higher o Java SDK/JRE 1.5.0 and 1.6.0_06 or higher	As appropriate
Java SDK/JRE	o Operating system	o N if the mid tier or Email Engine is installed. o N/A if the mid tier and Email Engine is not installed.	o Java SDK 1.5.0 and 1.6.0_06 or higher	As appropriate
An email exchange server	o Operating system	Y	o Any mail server using SMTP or MAPI standard protocols, such as Microsoft Exchange (Windows Server 2003)	As appropriate

Environment component	Dependencies	Optional Y/N	Version	Underlying environment
LDAP directory service	o Operating system	Y	o Any directory service using the LDAP standard protocol such as Microsoft Active Directory (Windows Server 2003)	As appropriate
Web browser	o BMC Remedy Mid Tier o AR System Server	o N if the mid tier installed. o N/A if the mid tier not installed.	o Microsoft Internet Explorer 6 or higher	As appropriate

Please refer to the ST for more technical details about the product and its associated security claims and functions.

6 Documentation

This section lists documentation that was used as evidence for the evaluation of BMC Remedy Action Request System 7.5.00 Patch 007 with BMC Remedy Encryption Security 7.5.00, English version. It contains these sections:

- Product Guidance
- Evaluation Evidence

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and therefore delivered with the TOE is as follows:

Note: The first document is Common Criteria-specific and is normative while the others are generally informative.

- BMC Remedy Action Request System 7.5.00 Common Criteria Supplemental Guide, October 2011
- BMC Remedy Action Request System 7.5.00 Mapping of Security Functional Requirements to Administrator and User Guidance, October 2011
- BMC Remedy Action Request System 7.5.00 Approval Server Guide, January 2009
- BMC Remedy Action Request System 7.5.00 Concepts Guide, January 2009
- BMC Remedy Action Request System 7.5.00 Configuration Guide, January 2009
- BMC Remedy Action Request System 7.5.00 C API Reference, January 2009
- BMC Remedy Action Request System 7.5.00 Database Reference, January 2009
- BMC Remedy Action Request System 7.5.00 BMC Remedy Distributed Server Option Guide, January 2009
- BMC Remedy Action Request System 7.5.00 BMC Remedy Email Engine Guide, January 2009
- BMC Remedy Action Request System 7.5.00 BMC Remedy Encryption Security Guide, January 2009
- BMC Remedy Action Request System 7.5.00 Error Messages Guide, January 2009
- BMC Remedy Action Request System 7.5.00 Form and Application Objects Guide, January 2009
- BMC Remedy Action Request System 7.5.00 BMC Remedy Flashboards Guide, January 2009
- BMC Remedy Action Request System 7.5.00 Introduction to Application Development with BMC Remedy Developer Studio, January 2009
- BMC Remedy Action Request System 7.5.00 Installation Guide, January 2009
- BMC Remedy Action Request System 7.5.00 Integration Guide, January 2009
- BMC Remedy Action Request System 7.5.00 Mid Tier Guide, January 2009

- BMC Remedy Action Request System 7.5.00 Optimizing and Troubleshooting Guide, January 2009
- BMC Remedy Action Request System 7.5.00 Workflow Objects Guide, January 2009
- BMC Remedy Action Request System 7.5.00 Master Index, January 2009

6.2 Evaluation Evidence

The following table identifies the additional documentation submitted as evaluation evidence by the vendor. With the exception of the Security Target, these documents are proprietary and not available to the general public.

Design Documentation	**Version**	**Date**
BMC Remedy Action Request System 7.5.00 Security Architecture Description	5.1	October 2011
BMC Remedy Action Request System 7.5.00 TOE Design and Functional Specification	7.1	October 2011

Lifecycle Documentation	**Version**	**Date**
BMC Remedy Action Request System 7.5.00 Lifecycle Support Guide	4.0	September 2011

Test Documentation	**Version**	**Date**
BMC Remedy Action Request System 7.5.00 Test Plans and Test Cases	4.0	September 2011

Security Target	**Version**	**Date**
BMC Remedy Action Request System 7.5.00 Security Target	1.10	October 2011

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for BMC Remedy Action Request System 7.5.00. It contains these sections:

- Developer Testing
- Evaluation Team Independent Testing
- Penetration Testing

Evaluation team testing was conducted at the vendor's development site in San Jose, California during the week of 29 August through 2 September, 2011.

7.1 Developer Testing

The developer created test procedures specifically to fulfill the test requirements for an EAL4 evaluation. The tests were developed to provide good coverage of the security functions related to each of the security requirements in the Security Target. The developer has documented their tests in a test plan where the results of the tests are presented as prose conclusions, notes, screen shots, and summaries for each of the applicable test platforms.

7.2 Evaluation Team Independent Testing

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE (in two distinct but representative configurations) in accordance with the provided guidance, and exercised a representative subset of the developers test plan on equipment configured in the testing laboratory. Note that the final subset of developer tests exercised during independent testing consisted of all automated tests (representing about 45% of the developer tests) and about 32% of the manual test procedures (many of which were exercised on multiple distinct test configurations) selected to ensure coverage of the claimed security functions.

This effort involved installing and configuring the AR System components in their respective tiers on a representative subset of the supported operating systems. Subsequently, the evaluators exercised a subset of the available developer's test procedures for AR System. The subset of tests was selected in order to ensure that each of the claimed security functions was meaningfully sampled.

Also, the evaluators devised independent tests to ensure that start-up and shutdown operations were audited, to verify the claimed methods of audit storage, to verify that unsuccessful authentication attempts were audited, to verify that cryptographic functions were audited, to verify that resource access was audited, to verify that audit records were reviewable, to verify the claimed content of audit records, to verify that the correct cipher suites were used in cryptographic operations, to verify that communications with an LDAP server was encrypted, to verify the claimed methods of cryptographic key destruction, to verify correct enforcement of access policies on protected resources, to verify license-based access restrictions, to ensure proper access control on active links, to verify that a user with no permissions actually had no permissions, to ensure that authentication worked as described, to verify that password complexity requirements were enforced, to verify that passwords are not stored in plaintext, to verify that users cannot change other user's password (unless they are an administrator), to verify the default security protection of resources, to verify the default role permissions, to verify that expired passwords were enforced, to verify that distributed operations were distributed correctly, and to verify that impersonation operations resulted in audit records that reflect both the actual and impersonated user.

7.3 Penetration Testing

In addition to the use of developer provided and independently devised security functional tests, the evaluators also explored the possibility to penetrate or bypass the security mechanisms. Much of this work was based on analysis of the design, source code, and actual configuration information derived from the installed and configured products. However, the evaluators also devised some tests including scans of the installed products,for open ports as well as common vulnerabilities, (e.g., using Wikto), attempts to enter bad data to ensure input validation, attempts at account harvesting, web proxy manipulation, and also examination of actual network traffic between the client and server products

Given the complete set of test results from test procedures exercised by the developer and the sample of tests directly exercised by the evaluators, the testing requirements for EAL4 are fulfilled.

8 Evaluated Configuration

As identified in the BMC Remedy Action Request System 7.5.00 Security Target, Version 1.10, October 2011 the evaluated configuration consists of the following TOE components operating in conjunction with the subsequent operational environment components. Section 5.1 identifies the specific dependencies among the components and also identifies which of the components are optional in the evaluated configuration. Ultimately the guidance identified previously describes specifically how each of the identified components needs to be installed and used in order to operate the evaluated products in their evaluated configuration.

TOE Identification: BMC Remedy Action Request System 7.5.00 Patch 007 (AR System) with BMC Remedy Premium Encryption Security 7.5.00 or with BMC Remedy Performance Encryption Security 7.5.00 (English version)

- BMC Remedy Action Request System Server 7.5.00 (patch 007)
- BMC Remedy Approval Server 7.5.00 (patch 007)
- BMC Remedy Email Engine 7.5.00 (patch 007)
- BMC Remedy Flashboards Server 7.5.00 (patch 007)
- Action Request System External Authentication LDAP plug-in 7.5.00 (patch 007)
- Action Request System Database Connectivity plug-in 7.5.00 (patch 007)
- BMC Remedy Mid Tier 7.5.00 (patch 007)
- BMC Remedy Developer Studio 7.5.00 (patch 007)
- BMC Remedy User 7.5.00 (patch 007)
- BMC Remedy Data Import 7.5.00 (patch 007)
- BMC Remedy Alert 7.5.00 (patch 007)
- BMC Remedy Mid Tier Configuration Tool 7.5.00 (patch 007)
- BMC Remedy Encryption Security 7.5.00 products (no patch)
- BMC Remedy Distributed Server Option 7.5.00 (patch 007)
- BMC Remedy Assignment Engine 7.5.00 (patch 007)

Operational Environment Components:

Operating System

- Microsoft Windows Server 2003 (32- or 64-bit) or higher
- Sun Solaris 9 or higher

Database

- Oracle 10G (R2) or higher
- Microsoft SQL Server 2005 or higher

Web Server

- Microsoft Internet Information Server (IIS) 6 or higher
- Tomcat 5.5.28 or higher

Servlet Engine

- Tomcat 5.5.28 or higher
- Java SDK/JRE 1.5.0 and 1.6.0_06 or higher

Java SDK/JRE

- Java SDK/JRE 1.5.0 and 1.6.0_06 or higher

E-Mail

- Any mail server using SMTP or MAPI standard protocols, such as Microsoft Exchange (Windows Server 2003)

LDAP Directory Service

- Any directory service using the LDAP standard protocol such as Microsoft Active Directory (Windows Server 2003)

Web Browser

- Microsoft Internet Explorer 6 or higher

9 Results of the Evaluation

The evaluation was conducted based upon Version 3.1 Revision 3 of the Common Criteria (CC) and the Common Methodology for Information Technology Security Evaluation (CEM). A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an “EAL 4” certificate rating be issued for BMC Remedy Action Request System 7.5.00 Patch 007.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements (SARs) are listed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation of the TSF
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures and automation
ALC_CMS.4	Problem tracking configuration management (CM) coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.2	Testing: security enforcing modules
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.3	Focused vulnerability analysis

10 Validator Comments and Recommendations

1. The product supports the ability to allow requests to be submitted or modified via e-mail. However, as such requests require the associated user to be identified and authenticated, those messages necessarily contain identifying and authenticating information. However, since the TOE does not support secure e-mail protocols, this feature must not be used in the evaluated configuration to avoid the unintentional or inappropriate disclosure of sensitive user credentials.

2. While there was no explicit conclusion or examination of STIG compatibility during the evaluation, the developer and evaluators have asserted a belief that identified components in the TOE operating environment could be configured to comply with applicable STIGs without affecting the operational of the TOE security functions.

3. The Validator has recommended that additional security claims seemingly could have been made (e.g., FTA_SSL.4), but the developer has elected to avoid extending the security claims for the evaluation as such the user should be aware that there do seem to be at least some minor security functions that have gone unchecked during the evaluation – the evaluation was essentially limited to the claims in the evaluated ST.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is BMC Remedy Action Request System 7.5.00 Security Target, Version 1.10, October 2011.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 3, July 2009.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 3, July 2009.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009.

[5] BMC Remedy Action Request System 7.5.00 Security Target, Version 1.10, October 2011.

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 September 2008.

[7] Evaluation Technical Report For BMC Remedy Action Request System 7.5.00, part 1 (and associated test report), version 0.3, 17 October 2011.

[8] Evaluation Technical Report For BMC Remedy Action Request System 7.5.00, part 2 (and associated test report), version 0.2, 9 September 2011