National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Marimba Client and Server Management from BMC Software Release 6.0.3

Report Number: CCEVS-VR-07-0046
Dated: 21 June 2007
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 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

List of Tables

1 Executive Summary

The evaluation of **Marimba Client and Server Management from BMC Software Release 6.0.3** was performed by SAIC, in the United States and was completed in May 2007. The evaluation was carried out in accordance with the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The criteria against which the BMC Marimba TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.2 and International Interpretations effective on 01, January 2007. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2.

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is EAL 3 family of assurance requirements. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Marimba Client and Server Management from BMC Software Release 6.0.3 Security Target.

This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is a software-only product that relies on underlying operating system and Java Virtual Machine services as well as the services of a LDAP server within the execution environment of the TOE. It should be understood that the evaluation involved only the analysis of the TOE and its interactions with its environment, but did not include analysis of the operation of any of those components supporting the TOE. The evaluation has been conducted in accordance with the provisions of the NIAP CCEVS and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the BMC Marimba product by any agency of the US Government and no warranty of the product is either expressed or implied.

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 successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Evaluation Technical Report For the BMC Software Marimba Client and Server Management (ETR) Parts 1 and 2 and the associated test report produced by SAIC.

1.1 Evaluation Details

Evaluated Product: Marimba Client and Server Management from BMC Software Release 6.0.3:

- Marimba® Control Center by BMC Software 6.0.3 SP2, with SSL enabled, and Publisher and Channel Copier versions 4.6.2, Logging Service 5.0.1 and Policy Service 5.1

- Marimba® Patch Management by BMC Software 6.5
- Marimba® Content Management by BMC Software with Content Replicator 6.5
- Marimba® Desktop/Mobile Application Management by BMC Software with Application Packager 6.5
- Marimba® Server Application Management by BMC Software with Application Packager 6.5
- Marimba® Desktop OS Management by BMC Software 6.0.3
- Marimba® Server OS Management for Unix and Linux by BMC Software 6.0.3

Note that each component of the TOE has a specific identifier and version, as indicated above, and which can be reviewed prior to copying and installing them (from the BMC product distribution site) and subsequently after the TOE is installed. While each component could be updated as newer versions become available, or a newer component could be installed initially, the user of the TOE should be aware that only the specific components identified above have been subject to evaluation.

Sponsor & Developer:	BMC Software, Inc. 2101 City West Blvd. Houston, Texas 77042
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Completion Date:	May 2007
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.2
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation, Version 2.2
Evaluation Class:	EAL 3
Description	The Marimba Client and Server Management TOE is a family of Desktop and Server Management products, which provide configuration management services for client devices. The Marimba Client and Server Management products are capable of deploying and maintaining a wide variety of information, called packages, whether it is individual files or documents, entire software suites, JAVA applications, or

	web sites.
Disclaimer	The information contained in this Validation Report is not an endorsement of the Marimba Client and Server Management product by any agency of the U.S. Government and no warranty of the Marimba Client and Server Management product is either expressed or implied.
PP:	none
Evaluation Personnel	Arnold, James Floyd, Craig
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

The Evaluation Team determined that there were no Interpretations applicable to this evaluation.

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 1– Threats

T.ACCESS	Unauthorized user	Access to TOE functions and data
T.AUDIT_CORRUPT	User accountability	Tamper with the audit trail
T. DISCLOSURE_OF_ CERTIFICATES	Protected network communication	Access to certificates to spoof a server
T.DISCLOSURE_OF_ COMMUNICATION	Protected network communication	Access to network traffic
T.DISCLOSURE_OF_ PRIVATE_KEYS	Protected network communication	Access to keys used to protect traffic
T. PRIVILEGE	Unauthorized user	Access to protected user data

2 Identification

The NIAP CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (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 EAL 4 in accordance with 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.

The following table serves to identify the evaluated Security Target and TOE:

Table 2 – ST and TOE identification

ST Title:	Marimba Client and Server Management from BMC Software Release 6.0.3 Security Target, version 2.3.0, 4 June 2007
TOE Identification:	• Marimba® Control Center by BMC Software 6.0.3 SP2, with SSL enabled, and Publisher and Channel Copier versions 4.6.2, Logging Service 5.0.1 and Policy Service 5.1 • Marimba® Patch Management by BMC Software 6.5 • Marimba® Content Management by BMC Software with Content Replicator 6.5 • Marimba® Desktop/Mobile Application Management by BMC Software with Application Packager 6.5 • Marimba® Server Application Management by BMC Software with Application Packager 6.5 • Marimba® Desktop OS Management by BMC Software 6.0.3 • Marimba® Server OS Management for Unix and Linux by BMC Software 6.0.3
CC Conformance:	• Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, January 2004, ISO/IEC 15408-2. • Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.2, January 2004, ISO/IEC 15408-3.
PP Conformance:	None
Assurance Level:	Evaluation Assurance Level 3
Operating Platform:	Various operating system platforms running Java Runtime Environment (JRE) version 1.3.1.10.

3 Security Policy

The following table identifies the policies implemented by the TOE:

Table 3 – Policies

P.ACCOUNTABILITY	All users of the system shall be held accountable for their security relevant actions within the system.
P.MANAGE	The system must provide authorized administrators with utilities to effectively manage the security functions of the TOE.

4 Assumptions

4.1 Physical Assumptions

The following physical assumptions are identified in the Security Target:

Table 4 – Personnel Assumptions

A.CONNECT	Any network resources used for communication between TOE components will be adequately protected from unauthorized access.
A.PROTECT	The components of TOE software critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.

4.2 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

Table 5 – Physical Assumptions

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance.
A.PLATFORM_REQUIREMENTS	The administrative personal have followed the instructions provided in the administrative guidance that recommend minimum hardware and software requirements on which the TOE operates. The administrative personal have configured the computer system on which the TOE is operating based on instructions in the administrative guidance.

4.3 Operational Assumptions

The following operational assumptions are identified in the Security Target:

Table 6 – Operational Assumptions

A.OPERATE_CORRECTLY	The computer platforms and operating systems in the environment are operating in a generally defect-free manner and follow either the manufacturers specifications, or accepted industry standards such as the secure sockets layer (SSL) protocol.
A.IDENT	The operating environment will provide a method of identification and authentication.
A.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives.
A.SYSPROTECT	The operating environment will provide protection to the TOE and its related data.
A.TIME	The operating environment will provide reliable system time.

5 Architectural Information

See section 2, and in particular section 2.4.1, of the Marimba Client and Server Management from BMC Software Release 6.0.3 Security Target, version 2.3.0, 4 June 2007 for a summary of the TOE and its architecture.

Note that the TOE includes the use of SSL to protect its communications. This instance of SSL is implemented using the BSAFE SSL-C 2.5.1 library technology from RSA Security, Inc.

6 Documentation

Following is a list of end-user documents supplied by the developer for the TOE:

- Marimba Documentation Addendum for the BMC Marimba Product Line NIAP Certification, version 6.0.3 (070302)
- Release Notes, version 6.0.3SP2 (051031)
- Marimba Documentation Addendum, version 3.0 (051031)
- Application Packager Administrator's Guide, version 6.5 (050513)
- Certificate Manager Help, version 4.6.1 (020628)
- Channel Copier Help, version 4.6.1 (030610)
- Content Replicator Release Notes, version 6.5 (051031)
- Deployment Guide, version 6.0.3, Patch Management 2.0.1 (051031)
- Infrastructure Administrator's Guide, version 6.0.3 (050331)
- Introduction to Marimba Products, September 2004, (040916)
- Marimba Reference, version May 2005, (050513)
- Patch Management Administrator's Guide, version 6.5, (0501031)
- Patch Management Deployment and Upgrade Guide, version 6.5 (051031)

- Release Notes Patch Management, version 6.5 (051031)
- Release Notes Application Packager version 6.5, 5/13/05
- Release Notes Controlled Availability Version 6.5 (051031)
- Release Notes Marimba OS Management, 3/31/05
- Planning Guide, version 6.0 (031219)
- Policy Management Administrator's Guide, version 6.0.3 (050331)
- Publisher Help, version 4.6.1, (020628)
- Report Center Administrator's Guide, version 6.0.3 (050331)
- Server Management Administrator's Guide, version 6.0.3 (050331)
- Server Management Advanced Topics Guide, version 6.0.3 (041207)
- Server Management Guide to the Command Line Interface, version 6.0.3 (041207)
- System Requirements for Marimba Products, version 6.0.3, Patch Management 2.0.1 (050414)

The security target used is:

- Marimba Client and Server Management from BMC Software Release 6.0.3 Security Target, version 2.3.0, 4 June 2007

7 IT Product Testing

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an EAL3 evaluation.

7.1 Developer Testing

Vendor testing is oriented toward security functional requirements; the documentation includes a test plan describing test approach, test configuration, test procedures, and test coverage. Each test procedure is further broken out into test cases that target specific security behavior associated with a security functional requirement (SFR). The evaluation team found the vendor test suite to be sufficiently broad in scope, addressing each of the security functional requirements in combination with the related external interfaces.

7.2 Independent Testing

The evaluation team exercised all of the developer's manual test procedures, and reused the team tests from the earlier evaluation effort.

The test configuration consisted of two TOE server instantiations, each configured per the defined evaluated configuration for the suite of BMC Marimba applications. That is, the test configuration consisted of a single test environment, which included two TOE instances:

- One running on Microsoft Windows Server 2003
- One running on Sun Microsystems Solaris 9

An additional platform was required to host the following server products. These are not part of the TOE, but are in the IT Environment, and are required to execute the test scripts.

- Microsoft SQL Server 2000 (MS SQL), running on Windows Server 2003

- Sun One Directory Server (i.e., LDAP) version 5.1, running on Windows Server 2003

MS SQL is the central repository for recording and reporting on audit records. The LDAP server provides password authentication services and provides user group functionality for role and Access Control List (ACL) support.

The evaluators installed the TOE according to the installation guidance and subsequently used the user and administrator guidance documents while performing tests.

Once the test configurations were established, the evaluator executed all (i.e., 100%) of the developer's tests (scripts and manual procedures) on the Windows platform, in each case getting the expected results as documented by the developer.

Only a portion of the manual tests were executed on the Solaris platform, given limited time available to test. In total, the evaluators exercise about 20% of the manual test procedures and 80% of the test scripts on the Solaris platform and the tests were selected such that at least some tests for each claimed security functions were exercised on the Solaris platform to ensure the TOE seemed to behave the same on each platform in relation to each claimed security function. Given evaluation results demonstrating that the developer had run all the tests on the applicable configurations and that the TOE application runs in a JVM as opposed to being natively compiled for each platform, the evaluators did not find it necessary to comprehensively exercise the available test procedures on every applicable platform.

The evaluation team implemented additional tests to extend the developer's testing and those tests are documented in the evaluation team test report. The evaluators based their tests on historical test from previous evaluations of this product with emphasis on new security claims made for this version of the product.

8 Evaluated Configuration

The evaluated configuration is a single instance of the Marimba Client and Server Management server and from BMC Software that is comprised of the following components operating in the context of a Windows, Solaris, or Red Hat Linux[1] operating system:

- Marimba® Control Center by BMC Software 6.0.3 SP2, with SSL enabled, and Publisher and Channel Copier versions 4.6.2, Logging Service 5.0.1 and Policy Service 5.1
- Marimba® Patch Management by BMC Software 6.5
- Marimba® Content Management by BMC Software with Content Replicator 6.5
- Marimba® Desktop/Mobile Application Management by BMC Software with Application Packager 6.5

[1] The specific supported operating systems include Windows NT 4.0, Windows 2000, Windows XP Professional, Windows 2000 and 2003 Server, Solaris 8 and 9, and Red Hat Linux AS 2.1 and AS 3.0. Note that while the evaluation team performed hands-on testing only on Windows Server 2003 and Solaris 9, the applications are JAVA based and the same application runs on all of the platforms identified above.

- Marimba® Server Application Management by BMC Software with Application Packager 6.5
- Marimba® Desktop OS Management by BMC Software 6.0.3
- Marimba® Server OS Management for Unix and Linux by BMC Software 6.0.3

9 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL3 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. 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. Verdicts were not assigned to assurance classes.

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

Table 7 – EAL3 Assurance Components

Assurance Class	Assurance Components
Configuration Management (ACM)	Authorization controls (ACM_CAP.3)
	TOE CM coverage (ACM_SCP.1)
Delivery and Operations (ADO)	Delivery procedures (ADO_DEL.1)
	Installation, generation, and start-up procedures (ADO_IGS.1)
Development (ADV)	Informal functional specification (ADV_FSP.1)
	Security enforcing high-level design (ADV_HLD.2)
	Informal correspondence demonstration (ADV_RCR.1)
Guidance Documents (AGD)	Administrator guidance (AGD_ADM.1)
	User guidance (AGD_USR.1)
Life Cycle Support (ALC)	Identification of security measures (ALC_DVS.1)
Tests (ATE)	Analysis of coverage (ATE_COV.2)
	Testing: high-level design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)

Assurance Class	Assurance Components
Vulnerability Assessment (AVA)	Examination of guidance (AVA_MSU.1)
	Strength of TOE security function evaluation (AVA_SOF.1)
	Developer vulnerability analysis (AVA_VLA.1)

10 Validator Comments/Recommendations

The Validation Team agreed with the conclusion of the SAIC CCTL Evaluation Team, and recommended to CCEVS Management that an EAL3 certificate rating be issued for the Marimba Client and Server Management from BMC Software Release 6.0.3.

11 Annexes

Not applicable.

12 Security Target

Marimba Client and Server Management from BMC Software Release 6.0.3 Security Target, version 2.3.0, 4 June 2007.

13 Acronym List

ACL – Access Control List
CC – Common Criteria
CEM – Common Evaluation Methodology
CCEVS – Common Criteria Evaluation and Validation Scheme
CCTL – Common Criteria Testing Laboratory
EAL – Evaluation Assurance Level
ETR – Evaluation Technical Report
HTML – Hypertext Markup Language
IT – Information Technology
JVM – Java Virtual Machine
LDAP – Lightweight Directory Access Protocol
NIAP – National Information Assurance Partnership
NIST – National Institute of Standards and Technology
NSA – National Security Agency
NVLAP – National Voluntary Laboratory Assessment Program
SSL – Secure Socket Layer
SAIC – Science Applications International Corporation
SFR – Security Functional Requirement
ST – Security Target
TOE – Target of Evaluation

Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): http://niap-ccevs.org/cc-scheme/.
- Science Applications International Corporation (SAIC) (http://www.saic.com).
- BMC Software, Inc. (http://www.bmc.com).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.3, August 2005.
- [CCEVS4] Guidance to Common Criteria Testing Laboratories, Draft, Version 1.0, March 2001.

Other Documents

- [ST] Marimba Client and Server Management from BMC Software Release 6.0.3 Security Target, version 2.3.0, 4 June 2007.