Certification Report

BMC Real End User Experience Monitoring and Analytics 2.5

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment, 2015

Document number: 383-4-261-CR
Version: 1.0
Date: 19 March 2015
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 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 19 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 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;
- Oracle and Java are registered trademarks of Oracle; and
- UNIX is a registered trademark of The Open Group.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

BMC Real End User Experience Monitoring and Analytics 2.5 (hereafter referred to as BMC EUEM), from BMC Software Inc., is the Target of Evaluation. The results of this evaluation demonstrate that BMC EUEM meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

BMC EUEM uses a technology called packet capture analysis to passively watch actual transactions from real users as they interact with a web application. Real User Collector devices capture user sessions in real time and Real User Analyzer devices report on errors and slow performance to help Web Operations teams fix problems when they occur. This process is commonly referred to as End-User Experience Monitoring (EUEM).

BMC EUEM is substantially different from traditional approaches to performance monitoring. The system does not generate any traffic. Instead, it reads a copy of traffic from the wire, assembles what it sees into requests for objects, pages, and user sessions, and records the performance and success (or failure) of these transactions.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 19 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 EUEM, 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 EUEM 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 Real End User Experience Monitoring and Analytics 2.5 (hereafter referred to as BMC EUEM), from BMC Software Inc..

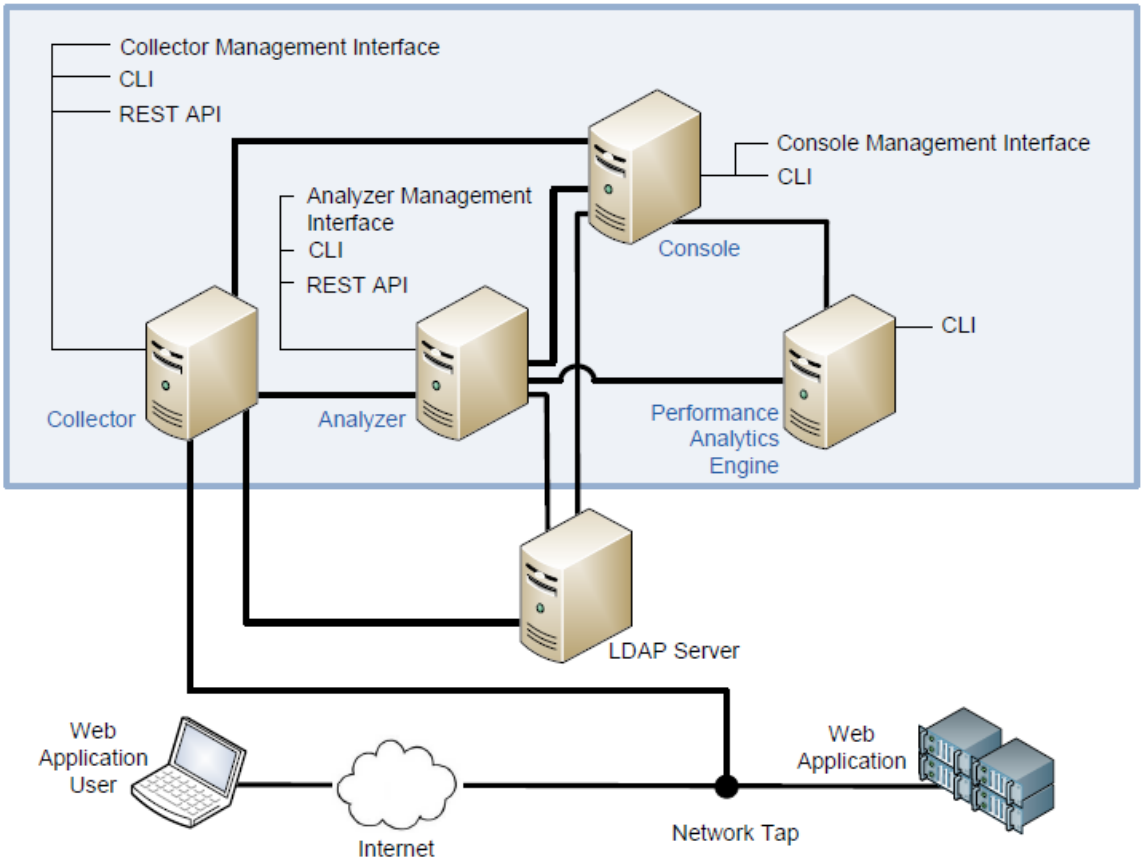
2 TOE Description

BMC EUEM uses a technology called packet capture analysis to passively watch actual transactions from real users as they interact with a web application. Real User Collector devices capture user sessions in real time and Real User Analyzer devices report on errors and slow performance to help Web Operations teams fix problems when they occur. This process is commonly referred to as End-User Experience Monitoring (EUEM).

BMC EUEM is substantially different from traditional approaches to performance monitoring. The system does not generate any traffic. Instead, it reads a copy of traffic from the wire, assembles what it sees into requests for objects, pages, and user sessions, and records the performance and success (or failure) of these transactions.

A diagram of the BMC EUEM architecture is as follows:

BMC EUUM TOE Boundary



3 Security Policy

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

- *Security Audit;*
- *User Data Protection;*
- *Identification and Authentication;*
- *Security Management; and*
- *User session data collection and reporting.*

4 Security Target

The ST associated with this Certification Report is identified below:

BMC Real End User Experience Monitoring and Analytics 2.5 Security Target, v0.07, 5 March 2015

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 EUEM 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:*
   - FCR_COL_EXT collection of user session data; and
   - FCR_REP_EXT reporting of user experience.

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 EUEM 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:

- 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 for audit record generation; and
- The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical and network access.

7 Evaluated Configuration

The evaluated configuration for BMC EUEM comprises:

- BMC Application Performance Management Console v 2.5.01 build 2.5.66.300;

- BMC Real User Collector v 2.5.01 build 2.5.66.300;
- BMC Real User Analyzer v 2.5.01 build 2.5.66.300; and
- BMC Performance Analytics Engine v 2.5.01 build 2.5.66.300.

running on ESXi 5.5 on a general purpose VMWare supported server platform.

The publication entitled BMC Real End User Experience Monitoring 2.5, 20 February 2014 describes the procedures necessary to install and operate BMC EUEM in its evaluated configuration.

8 Documentation

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

a. *BMC Real End User Experience Monitoring 2.5, 20 February 2014.*

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of BMC EUEM, including the following areas:

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

The evaluators reviewed the flaw remediation procedures used by developer for the BMC EUEM. 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;

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 Security Target;

c. Enforcing Password Policy: The objective of this test goal is to confirm that the strict password policy is being enforced and any non-conformance is audited; and

d. User Security Rules:

    a. Assign Security Roles: The objective of this test goal is to confirm that a user can be assigned different roles and that the results are audited;

    b. Modify Security Roles: The objective of this test goal is to confirm that user roles can be modified and that the modifications are audited.

[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.

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;
    a. Use nmap to scan for services running on open ports;
    b. Use Nexpose to scan for potential vulnerabilities, including Denial of Service;
    c. Use Internet Search engines to identify potential vulnerabilities;
b. Information Leakage verification: The objective of this test goal is to monitor for data leakage during start up, shut down and login and any other place where one component is communicating with the other; and
c. Concurrent Logins: The objective of this test case is to confirm that concurrent logins does not cause the TOE to malfunction.

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

10.4 Conduct of Testing

BMC EUEM 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 EUEM behaves as specified in its ST and functional specification.

11 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.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
API	Application Programming Interface
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
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
REST API	Representational State Transfer Application Programming Interface
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 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 Real End User Experience Monitoring and Analytics 2.5 Security Target, v0.07, 5 March 2015

e. Evaluation Technical Report for BMC Real End User Experience Monitoring and Analytics 2.5, v1.0, 19 March 2015.