Certification Report

BMC Atrium® Discovery and Dependency Mapping 10.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-259-CR
Version: 1.1
Date: 10 February 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 10 February 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 registered trademark:

- BMC Atrium® is a registered trademark of BMC Software, Inc.

TABLE OF CONTENTS

Executive Summary

BMC Atrium® Discovery and Dependency Mapping 10.0 (hereafter referred to as BMC Atrium® Discovery), from BMC Software, Inc., is the Target of Evaluation (TOE). The results of this evaluation demonstrate that BMC Atrium® Discovery meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

BMC Atrium® Discovery is a software-only TOE that is provided to customers as a virtual appliance in the Open Virtualization Format. The TOE automatically discovers physical and virtual servers, applications, and network devices and correlates the relationships between them.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 10 February 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 Atrium® Discovery, 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 Atrium® Discovery 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).

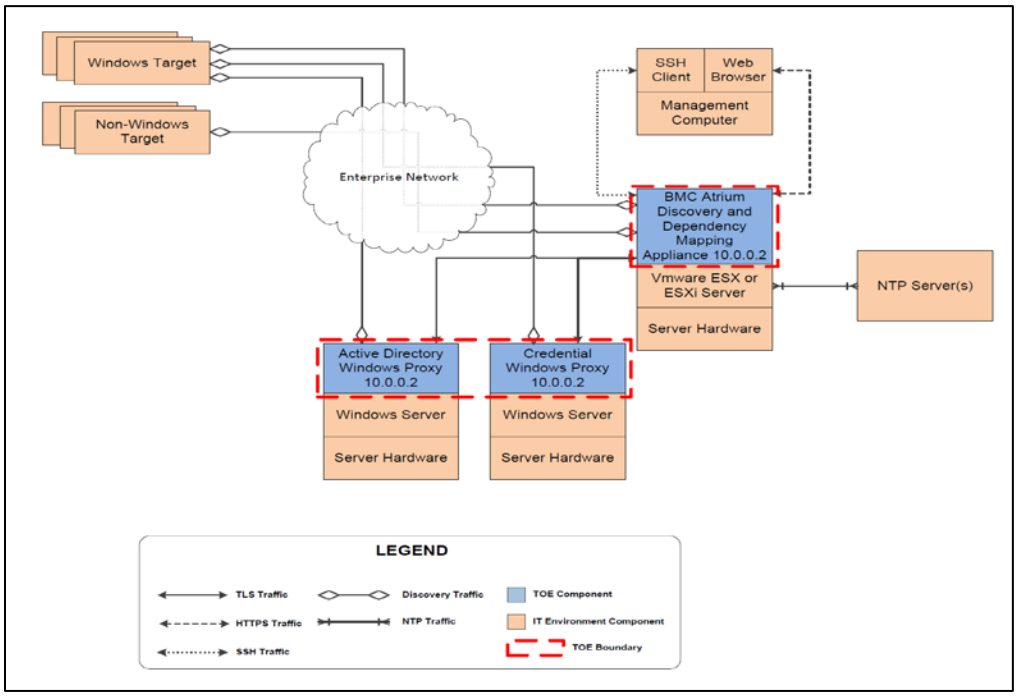
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is BMC Atrium® Discovery and Dependency Mapping 10.0 (hereafter referred to as BMC Atrium® Discovery), from BMC Software, Inc..

2 TOE Description

BMC Atrium® Discovery is a software-only TOE that is provided to customers as a virtual appliance in the Open Virtualization Format. The TOE automatically discovers physical and virtual servers, applications, and network devices and correlates the relationships between them. The TOE uses an agent-less approach to build a complete topology of applications and infrastructure, including servers, operating systems, software, network devices, business applications, and dependencies, and updates the topology as often as needed. For more detailed discovery of Windows-based platforms, the TOE employs a Windows proxy installed on a Windows system. The TOE includes two cryptographic modules that are used to secure communications between the TOE components and between the TOE and the IT environment.

A diagram of the BMC Atrium® Discovery architecture is as follows:



3 Security Policy

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

- *Security Audit*
- *Cryptographic Support*
- *User Data Protection*
- *Identification and Authentication*
- *Security Management*
- *Protection of the TOE Security Functionality*
- *Trusted Path/Channels*
- *Discovery and Dependency Mapping*

The following cryptographic module was evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate**
OpenSSL FIPS Object Module	1747
Red Hat Enterprise Linux 6.6 OpenSSL Module (RPM file 1.0.1e-30.el6_6.4)	2441

4 Security Target

The ST associated with this Certification Report is identified below:

BMC Atrium Discovery and Dependency Mapping 10 Security Target version 0.12, 10 February 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 Atrium® Discovery 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:*
    - DDM_DIS.1- Discovery
    - DDM_DEP.1 - Determine Dependency Relationships

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 Atrium® Discovery 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 authorized administrators will be assigned to install, configure and manage the TOE and the security of the information it contains.*
- *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 TOE will be installed in a manner that will limit physical access to authorized users.*
- *All supporting operational environment components have had all current security patches (if applicable) applied, and the Administrator has configured the inherent component security mechanisms to their most restrictive settings that will still permit TOE functionality and interoperability. Any such patch must not interfere with the correct functioning of TOE's interfaces to the supporting operational environment components.*
- *The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical access.*
- *The operational environment will provide reliable system time to the TOE.*

7 Evaluated Configuration

The evaluated configuration for BMC Atrium® Discovery comprises:

- BMC Atrium Discovery and Dependency Mapping Appliance 10.0.0.2 build 365935 with Operating System update 6.14.11.21 running on VMware ESXi 4.1 and VMware ESXi 5.5
- BMC Atrium Discovery and Dependency Mapping Windows Proxy 10.0.0.2 build 365935 with Operating System update 6.14.11.21running on Windows Server 2008 R2

The publication entitled *BMC Atrium® Discovery and Dependency Mapping 10.0 Guidance Supplement, Version 0.04, February 2015* describes the procedures necessary to install and operate BMC Atrium® Discovery in its evaluated configuration.

8 Documentation

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

a. BMC Atrium Discovery Release Notes, March 2014;

b. BMC Atrium® Discovery and Dependency Mapping 10.0 Guidance Supplement Version 0.04, February 2015;

c. Getting Started with BMC Atrium Discovery, March 2014;

d. BMC Atrium Discovery User Guide, March 2014;

e. BMC Atrium Discovery Configuration Guide, March 2014;

f. BMC Atrium Discovery Deployment Guide, March 2014;

g. BMC Atrium Application Mapping Guide, March 2014;

h. Security in BMC Atrium Discovery, March 2014; and

i. Troubleshooting, March 2014.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of BMC Atrium® Discovery, including the following areas:

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

The evaluators reviewed the flaw remediation procedures used by developer for the BMC Atrium® Discovery. 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; and

b. Password Re-Use History: The objective of this test goal is to verify that the rules for password re-use are enforced by the TOE.

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. Concurrent Logins: The objective of this test goal is to confirm that concurrent logins will not cause the TOE to malfunction; and

c. Session Management: The objective of this test goal is to confirm that the BMC Atrium® Discovery web user interface cannot be bypassed.

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

[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.

10.4 Conduct of Testing

BMC Atrium® Discovery 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 Atrium® Discovery 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 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
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
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 Atrium Discovery and Dependency Mapping 10 Security Target version 0.12, 10 February 2015.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation for BMC Software, Inc. BMC Atrium® Discovery and Dependency Mapping 10.0 Document No. 1815-000-D002-B, Version 1.2, 10 February 2015.