Certification Report

EAL 2+ Evaluation of Infoblox® NetMRI® v4.2.2.45

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-119-CR
Version: 1.0
Date: 12 May 2010
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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply 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 Canada, 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 Canada, 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 Canada.

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, 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 located in Ottawa, 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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 12 May 2010, 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 trademarked or registered trademarks:

- VMware is a registered trademark or trademark of VMware Incorporated;.
- Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation; and
- Mozilla and Firefox are registered trademarks of the Mozilla Foundation.

TABLE OF CONTENTS

Executive Summary

The Infoblox® NetMRI® v4.2.2.45 (hereafter referred to as NetMRI), from Infoblox Incorporated, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

NetMRI is a Network Configuration and Change Management (NCCM) product. NetMRI automates network configuration, change, and compliance management by continuously monitoring, auditing, and verifying network device configurations. NetMRI identifies configuration problems and anomalies and provides remediation options. NetMRI includes policy rules and automated reporting to monitor, audit and verify compliance with published best practices.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 3 May 2010 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 the NetMRI, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security 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.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 2 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted 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 following augmentation is claimed: ALC_FLR.2 - Flaw reporting procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the NetMRI 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is Infoblox® NetMRI® v4.2.2.45 (hereafter referred to as NetMRI), from Infoblox Incorporated.

2 TOE Description

NetMRI is a Network Configuration and Change Management (NCCM) product. NetMRI automates network configuration, change, and compliance management by continuously monitoring, auditing, and verifying network device configurations. NetMRI identifies configuration problems and anomalies and provides remediation options. NetMRI includes policy rules and automated reporting to monitor, audit and verify compliance with published best practices.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the NetMRI is identified in Section 6 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Infoblox Inc. NetMRI® Version 4.2.2.45 Security Target
Version: 1.2
Date: 29 April 2010

5 Common Criteria Conformance

The evaluation was conducted 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*.

NetMRI is:

a) Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2;

b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c) Common Criteria EAL 2 augmented, with all security the assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 - Flaw reporting procedures.

6 Security Policy

NetMRI implements the Management Access Control Policy that controls user access to audit, network device configuration, and authentication data. In addition, NetMRI implements policies pertaining to security audit, identification and authentication, security management, protection of the TSF, and TOE access.

Further details on these policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of NetMRI 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- administrators are non-hostile, appropriately trained, and follow all administrator guidance.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- the environment will protect the TOE from unauthorized access.

7.3 Clarification of Scope

NetMRI offers protection against attackers possessing basic attack potential. NetMRI is not intended for situations which involve determined attempts by hostile or well-funded attackers possessing attack potential of enhanced-basic or beyond.

8 Architectural Information

NetMRI is a software-only TOE that comprises the NetMRI Application and the underlying NetMRI OS (operating system). Further details about the system architecture are proprietary to the vendor, and are not provided in this report.

9 Evaluated Configuration

There are two NetMRI versions: Virtual Appliance; and Physical Appliance. The Virtual Appliance version installs on VMware; the Physical Appliance version installs on Netcordia-

supplied hardware appliances. The evaluated configuration for NetMRI comprises Infoblox® NetMRI® v4.2.2.45 executing on the following VMware and Netcordia appliances:

VMware:

- VMware vSphere 4 (ESX/ESXi 3.5/4.0 managed hosts);
- VMware ESX/ESXi 4.0 (standalone);
- Virtual Center 2.5 managed ESX/ESXi 3.5 hosts;
- VMware ESX/ESXi 3.5 (standalone);
- VMware Workstation 6.51+;
- VMware Player 2.5.3+;
- VMware Server 2.0.1+;
- VMware ACE 2.5.3+; and
- VMware Fusion.

Appliances:

- Model: Campus Rackmount 7200rpm;
- Model: Campus Rackmount 10k rpm;
- Model: Small Enterprise Rackmount 7200rpm;
- Model: Large Enterprise Rackmount with SAS drives; and
- Model: NextGen Large Enterprise Rackmount.

NetMRI management workstation supported web browsers include: Microsoft Internet Explorer version 7; Microsoft Internet Explorer version 8; and Mozilla Firefox version 3.0+.

10 Documentation

The Netcordia documents provided to the consumer are as follows:

- NetMRI 4.2 User's Guide, January 21, 2010;
- NetMRI and Operations Center Deployment Guide For Software Version 4.x, February 19, 2010; and
- NetMRI v4.2.2.45 Guidance Documentation Supplement, Version 0.3, April 9, 2010.

11 Evaluation Analysis Activities

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

Development: The evaluators analyzed the NetMRI functional specification, design documentation, and security architecture description; they determined that the design completely and accurately describes the TSF interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the NetMRI security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the NetMRI 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 NetMRI configuration management system and associated documentation was performed. The evaluators found that the NetMRI configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of NetMRI during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Netcordia for NetMRI. 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.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of NetMRI. Additionally, the evaluators conducted a review of public domain vulnerability databases to identify possible potential vulnerabilities in the TOE. The evaluators identified potential vulnerabilities for testing applicable to the NetMRI in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 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[2].

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 and TOE design was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

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 was the following list of EWA-Canada test goals:

a) Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration by following all instructions in the developer's Installation and Administrative guidance;

b) Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator's TOE installation;

c) Identification and Authentication: The objective of this test goal is to ensure that the identification and authentication requirements have been met;

d) Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed;

e) Security Management: The objective of this test goal is to ensure the security management is correct; and

f) Basic Product Functionality: The objective of this test goal is to exercise the TOE's basic functionality.

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

12.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focused review of all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a) Misuse Testing: The objective of this testing is to determine the TOE's response to unexpected input and events, including user behaviour which could be accidental or intentional.

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

12.4 Conduct of Testing

NetMRI was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the developer's facility in Annapolis, MD, USA and at the Information Technology Security Evaluation and Testing (ITSET) Facility at EWA-Canada. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the NetMRI behaves as specified in its ST and functional specification.

13 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.

14 Evaluator Comments, Observations and Recommendations

The documentation for the NetMRI includes comprehensive user guidance; the NetMRI is straightforward to configure, use and integrate into a corporate network.

Netcordia, Inc has a well defined product development process. Configuration management (CM) and quality assurance (QA) provide the requisite controls for managing all CM/QA activities.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CM	Configuration Management
CPL	Certified Products List
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NCCM	Network Configuration and Change Management
PALCAN	Program for the Accreditation of Laboratories-Canada
QA	Quality Assurance
SAS	Serial Attached SCSI
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

16 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

d. Infoblox Inc. NetMRI® Version 4.2.2.45 Security Target, Revision No. 1.2, 29 April 2010.

e. Evaluation Technical Report for EAL 2+ Evaluation of Infoblox® NetMRI® v4.2.2.45, Document No. 1628-000-D002, Version 0.6, 3 May 2010, Common Criteria Evaluation Number: 383-4-119.