Certification Report

EAL 2 Evaluation of

CA Spectrum® Network Fault Manager r9 SP1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-113-CR
Version: 1.0
Date: 08 September 2009
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 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. 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, 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 located in Ottawa, Ontario.

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 08 September 2009, 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 at: http://www.cse-cst.gc.ca/its-sti/services/cc/cp-pc-eng.html and http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked or registered trademarks:

- CA is a trademark of CA.
- Spectrum is a registered trademark of CA.

TABLE OF CONTENTS

Executive Summary

CA Spectrum® Network Fault Manager r9 SP1 (hereafter referred to as Spectrum), from CA, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 evaluation.

Spectrum is a network management system that monitors the state of managed elements including devices, host systems and connections. Status information such as fault and performance data from these elements is collected and stored. Spectrum analyzes this information to track conditions within the network that it monitors. If an abnormal condition is detected, the event is analyzed and the appropriate users are alerted. Spectrum presents the user with possible causes and proposed solutions to the problem.

Spectrum:

- provides auditing of user actions;
- provides identification and authentication of its users;
- provides access control based on assigning security communities, privileges and rules to a specific user or to a group of which the user is a member; and
- provides management of user accounts and their security attributes.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 2 September 2009 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 Spectrum, 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 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.*

Communications Security Establishment Canada, as the CCS Certification Body, declares that Spectrum 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

[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.

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 Evaluation Assurance Level (EAL) 2 evaluation is CA Spectrum® Network Fault Manager r9 SP1 (hereafter referred to as Spectrum), from CA.

2 TOE Description

Spectrum is a network management system that monitors the state of managed elements including devices, host systems and connections. Status information such as fault and performance data from these elements is collected and stored. Spectrum analyzes this information to track conditions within the network that it monitors. If an abnormal condition is detected, the event is analyzed and the appropriate users are alerted. Spectrum presents the user with possible causes and proposed solutions to the problem.

Spectrum:

- provides auditing of user actions;
- provides identification and authentication of its users;
- provides access control based on assigning security communities, privileges and rules to a specific user or to a group of which the user is a member; and
- provides management of user accounts and their security attributes.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Spectrum is identified in Section 7 of the Security Target (ST).

4 Security Target

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

Title: CA Spectrum® Network Fault Manager r9 SP1 Security Target
Version: 1.5
Date: 14 August 2009

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.*

Spectrum 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 conformant*, with all security the assurance requirements in the EAL 2 package.

6 Security Policy

Spectrum implements the Spectrum Discretionary Access Control Policy to control the access of processes acting on behalf of users to event records stored by the TOE. Spectrum uses roles and the concept of a "security community" to manage the aggregation and assignment of access privileges to individual users and groups of users. Details of this security policy can be found in Section 7 of the ST.

In addition, Spectrum implements policies pertaining to security audit, identification and authentication and security management. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Spectrum 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 Assumptions are listed in the ST:

- An individual is appointed to act as the Super User for the TOE. This individual is responsible for initial installation and configuration of the TOE as well as performing patches and updates to the TOE and its operating environment when required.
- Administrators of the TOE (including the Super User) are not careless, willfully negligent nor hostile, and follow the guidance instructions provided with the TOE.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is physically protected from unauthorized modifications to its software.
- The network monitored by the TOE is isolated from other networks.

7.3 Clarification of Scope

In its evaluated configuration, the TOE is divided between two separate computers. The Spectrum Host computer (which may run on either the Windows 2003 Server SP2 or Solaris 10 operating systems) runs the TOE's server and database components. The Spectrum Client computer (which may also run on either the Windows 2003 Server SP2 or the Solaris 10 operating systems) runs the OneClick Console which provides remote administrative access to the TOE.

8 Architectural Information

The Spectrum Network Fault Manager r9.0 SP1 consists of two major components, the Spectrum Host and the Spectrum Client.

The Spectrum Host is a computer running either the Windows 2003 Server SP2 or the Solaris 10 operating systems. The following software components of the TOE execute on the Spectrum host:

- **SpectroSERVER**. SpectroSERVER is the primary server for the SPECTRUM product; it functions as a database server, modeling engine, and device manager. SpectroSERVER processes events, generates alarms, and tracks statistics concerning managed elements.

- **SpectroSERVER Database**. The SpectroSERVER relies on this object-oriented database which contains model types that define how a managed element is represented, and models that represent specific managed elements.

- **Archive Manager**. The Archive Manager is used to log and retrieve historical event records, which it provides to users via the Web Server when access to the stored information is requested.

- **Distributed Data Manager.** The Distributed Data Manager (DDM) database stores the logged historical event records of the elements which SPECTRUM manages on its monitored network. The DDM database is updated with the information which is sent to it via the Archive Manager.

- **Web Server.** The Tomcat Web Server contains two components: the OneClick Server and the Report Manager. The OneClick Server allows users from a remote machine to connect to the TOE to manage the TOE's users, access control features, and perform the TOE's network management capabilities on the models of elements within the network the TOE manages. Report Manager allows users generate up-to-date reports about the inventory, availability, performance, change and fault history of network assets managed by SPECTRUM.

- **Report Database**. The Report Database stores the information which the Report Manager extracts from the SpectroSERVER Database. This information is kept current by the Report Manager by extracting the information at regular intervals.

The Spectrum Client is a computer running either the Windows 2003 Server SP2 or the Solaris 10 operating systems. The Spectrum OneClick Console is installed on the client system. The OneClick Console is designed to deliver Spectrum information to remote users.

9 Evaluated Configuration

The evaluated configuration for Spectrum comprises:

a. A Spectrum Host computer running either the Windows 2003 Server SP2 or the Solaris 10 operating systems. The following software components are installed on the Spectrum Host computer;
   - SpectroServer;
   - SpectroServer Database;
   - Archive Manager;
   - Distributed Data Manager;
   - WebServer; and
   - Report Database.

b. A Spectrum Client computer also running either the Windows 2003 Server SP2 or the Solaris 10 operating systems. The following software components are installed on the Spectrum Client computer;
   - OneClick Console.

10 Documentation

The CA documents provided to the consumer are as follows:

- Spectrum Installation Guide, r9.0;
- Report Manager Installation and Administration Guide, Document 5169;
- Spectrum OneClick Administration Guide, Document 5166;
- OneClick Console User Guide, Document 5130;
- Spectrum Control Panel User Guide, Document 5029;
- Spectrum SpectroServer Performance Administration Guide r9.0; and
- Evaluated Configuration for CA Spectrum Network Fault Manager, R9.0 SP1, July 2009.

11 Evaluation Analysis Activities

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

Development: The evaluators analyzed the Spectrum 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 Spectrum security architectural description and determined that the initialization process was 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 were correct.

Guidance Documents: The evaluators examined the Spectrum preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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 were complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Spectrum configuration management system and associated documentation was performed. The evaluators found that the Spectrum 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 Spectrum during distribution to the consumer.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Spectrum. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Spectrum potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the Spectrum 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 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's 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 provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

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; and

e. Users and Roles: The objective of this test goal is to ensure the users and roles functionality is correct.

12.3 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:

- Reconnaissance;
- Port Scanning;

[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.

- Misuse; and
- Denial-of-service.

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

12.4 Conduct of Testing

Spectrum 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 (ITSET) Facility at EWA-Canada. 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.

12.5 Testing Results

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

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 2 **l**evel 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 complete documentation for Spectrum includes Installation, Administration, User and Performance guides.

The installation and configuration of Spectrum is straightforward and well described in the documentation.

CA's Configuration Management (CM) and Quality Assurance (QA) activities are well established and rigorously followed, thereby providing a solid foundation for all product development activities.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility

Acronym/Abbreviation/ Initialization	Description
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
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
QA	Quality Assurance
ST	Security Target
TOE	Target of Evaluation

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 2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

d. CA Spectrum Network Fault Manager r9 SP1 Security Target, Version 1.5, 14 August 2009.

e. Evaluation Technical Report for EAL 2 Common Criteria Evaluation of CA Spectrum Network Fault Manager r9.0 SP1, Version 1.0, 2 September 2009.