Certification Report

EAL 2+ Evaluation of EMC® CLARiiON® FLARE v4.29 with Navisphere v6.29

running on CX4 Series Storage Systems

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-120-CR
Version: 1.0
Date: 15 February 2010
Pagination: i to iv, 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 3.1R2,* for conformance to the *Common Criteria for IT Security Evaluation, Version 3.1R2*. 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, 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 15 February 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:

- CLARiiON® is a registered trademark symbol of EMC Corporation.
- EMC® is a registered trademark symbol of EMC Corporation.
- Microsoft, and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries,

TABLE OF CONTENTS

Executive Summary

The EMC® CLARiiON® FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems (hereafter referred to as the EMC CLARiiON), from EMC, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

The EMC CLARiiON is a software package designed to provide managed storage on a Storage Area Network (SAN) and is made up of two software components, FLARE and Navisphere, which comprise the TOE. The purpose of the TOE is to provide a storage system to the application servers attached to the SAN through the use of Logical Units (LUNs). The Security Management function of Navisphere allows Administrators to properly configure this functionality using roles, which grant access to view, create, or modify Storage Groups, RAID groups, LUNs, and even individual disk drives.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 8 January 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 EMC CLARiiON, 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 2.* The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

The Communications Security Establishment Canada, as the CCS Certification Body, declares that the EMC CLARiiON 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 EMC® CLARiiON® FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems (hereafter referred to as EMC CLARiiON), from EMC.

2 TOE Description

The EMC CLARiiON is a software package designed to provide managed storage on a SAN and is made up of two software components, FLARE and Navisphere, which comprise the TOE. The purpose of the TOE is to provide a storage system to the application servers attached to the SAN through the use of Logical Units (LUNs). The Security Management function of Navisphere allows Administrators to properly configure this functionality using roles, which grant access to view, create, or modify Storage Groups, RAID groups, LUNs, and even individual disk drives.

3 Evaluated Security Functionality

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

4 Security Target

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

Title: EMC Corporation EMC® CLARiiON® FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems Security Target
Version: 0.5
Date: 12 January 2010

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*.

The EMC CLARiiON 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, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

The following statements are representative of the Security Policy:

Authentication and Security Management. Users must authenticate to the EMC CLARiiON before being able to perform any TSF-mediated actions. A user authenticating to the EMC CLARiiON must provide a user name and password for a valid user account. The EMC CLARiiON implements role based security management. Roles are assigned to individuals at the time their user accounts are established.

Protection of User Data. All user data stored on the TOE is protected through the use of discretionary access control enforced on Subjects and Objects. A valid Subject[1] of the TOE is allowed to Read and Write to a LUN if the Subject and the LUN are members of the same Storage Group. Data integrity is protected through the use of RAID technology.

For further details on security policies, please refer to the ST.

[1] Note: A Subject is an attached server and not a human user.

7 Assumptions and Clarification of Scope

Consumers of the EMC CLARiiON product 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:

- There will be one or more appropriately trained and competent individuals assigned to manage the EMC CLARiiON and the security information it contains; and
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the EMC CLARiiON documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The array(s) upon which EMC CLARiiON is installed resides in a physically secure location and only authorized individuals are granted physical access to the host; and
- The environment will provide the TOE with reliable timestamps and Application Server identification and authentication security functionality.

7.3 Clarification of Scope

The EMC CLARiiON is intended for use by a non-hostile and well-managed user community. It relies on the environment to provide it physical and logical protection.

It is the responsibility of the Administrator to properly configure the environment of the Application Servers to provide accurate World Wide Names for Identification and Authentication, and a secure communications method between the Applications Servers and the SAN.

Product features and functionality that are not part of the evaluated configuration of the TOE are:

- CLARiiON CX4 storage appliance hardware
- iSCSI with Challenge-Handshake Authentication Protocol (CHAP) authentication
- Remotely Anywhere
- Navisphere Analyzer
- Navisphere SnapView
- Navisphere MirrorView/Asynchronous
- Navisphere MirrorView/Synchronous
- Navisphere SAN Copy
- Navisphere Quality of Service Manager (NQM)

8 Architectural Information

The software-only TOE is the EMC CLARiiON FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems which consists of a variety of purpose-built appliances.

The EMC FLARE software is a Storage Operating Environment (SOE) optimized for implementation of RAID storage architectures, providing fault-tolerance and data integrity. It enables the use of virtual storage elements or logical units (LUNs) to improve performance and capacity utilization. FLARE also implements a technology called Access Logix, which lets multiple hosts share a storage system by using Storage Groups. A Storage Group is one or more LUNs within a storage system that is reserved for one or more hosts and is inaccessible to other hosts. Access Logix enforces the host-to-Storage Group permissions.

Navisphere is a storage-system management application for configuring, monitoring, and managing EMC CLARiiON® storage systems. It resides on each storage system Storage Processor (SP) and is downloaded to the browser when the Storage Management Server software is accessed. The Navisphere application includes two major software subcomponents; the Storage Management Server and the Navisphere Manger (see details below). Navisphere provides the following basic functionality:

- Discovery and monitoring of CLARiiON storage systems
- Storage configuration and allocation

- Status and configuration information display
- Event management

The Storage Management Server software is provided with Navisphere and executes on each SP in a storage system, and performs the following functions:

- Receives and responds to requests from Navisphere Manager
- Forwards status and configuration updates to Navisphere Manager
- Replicates user and domain information to all storage systems in the storage domain
- Authenticates and authorizes users
- Logs all user logins and requests

Navisphere Manager is a web-based Graphical User Interface (GUI) to the Navisphere application that provides for the secure management of CLARiiON® storage systems using a common browser. Many of the management functions can also be accomplished using the Navisphere Secure Command Line Interface (CLI), a set of commands that can be executed in non-graphical environments. Access to these management interfaces is controlled by an authentication function that allows for user accounts defined within Navisphere.

9 Evaluated Configuration

The TOE is software-only defined as:

- EMC® CLARiiON® FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems .

The TOE includes the following software builds:

- FLARE v4.29.000.005.003, and
- Navisphere v6.029.000.006.034.

The TOE is deployed on the following CX4 Series Storage Systems:

- CX4 Model 120,
- CX4 Model 240,
- CX4 Model 480, and
- CX4 Model 960.

10 Documentation

The EMC documents provided to the consumer are as follows:

a. EMC Navisphere Manager Online Help 6.29;

b. EMC Navisphere Analyzer Command Line Interface (CLI) Reference;

c. EMC Navisphere Command Line Interface (CLI) Reference;

d. EMC CX4 Series FLARE Operating Environment Version 04.29 Release Notes;

e. EMC CLARiiON CX4-(120/240/480/960) Setup Guide(s);

f. EMC Navisphere Analyzer Version 6.29.00 Release Notes;

g. EMC Navisphere Manager Version 6.29.00 Release Notes;

h. EMC Navisphere Host Agent/CLI and Utilities Release Notes; and

i. CLARiiON FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems Guidance Documentation Supplement, v0.2, 4 January 2010.

11 Evaluation Analysis Activities

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

Development: The evaluator analyzed the EMC CLARiiON functional specification and design documentation, and 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 evaluator analyzed the EMC CLARiiON security architectural description and determined that the initialization process was secure and that the security functions are protected against tamper and bypass. The evaluator also independently verified that the correspondence mappings between the design documents were correct.

Guidance Documents: The evaluator examined the EMC CLARiiON 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 evaluator 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 EMC CLARiiON configuration management system and associated documentation was performed. The evaluator found that the EMC CLARiiON 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 evaluator examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of EMC CLARiiON during distribution to the consumer.

The evaluator reviewed the flaw remediation procedures used by EMC for EMC CLARiiON. During a site visit, the evaluator also examined the evidence generated by adherence to the procedures. The evaluator 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 evaluator conducted an independent vulnerability analysis of EMC CLARiiON. Additionally, the evaluator conducted a review of public domain vulnerability databases. The evaluator did not identify any potential vulnerabilities applicable to the EMC CLARiiON 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 evaluator 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 evaluator 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:

[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.

a. 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 TOE Description of the Security Target, 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; and

c. Independent Evaluator Testing: The objective of this test goal is to exercise the TOE's claimed functionality through evaluator independent testing and to augment any areas that were not covered during the repeat of developer testing.

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:

a. Generic vulnerabilities;
b. Bypassing;
c. Tampering; and
d. Direct attacks.

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

12.4 Conduct of Testing

EMC CLARiiON was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the developer's QA facility in Westborough, Massachusetts to leverage the existing lab and available hardware. The CCS Certification Body pre-approved the draft test plan and has previously witnessed independent testing at this location by an EWA-Canada evaluator. 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 EMC CLARiiON behaves as specified in its ST, functional specification, TOE design, and security architecture description.

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 complete documentation for the EMC® CLARiiON® FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems includes a comprehensive Installation and Administration Guide (See Section 10).

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
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CHAP	Challenge-Handshake Authentication Protocol
CPL	Certified Products list
CM	Configuration Management
CLI	Command Line Interface
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
iSCSI	Internet Small Computer System Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LUN	Logical Unit
NQM	Navisphere Quality of Service Manager
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SFP	Security Function Policy
SP	Storage Processor

Acronym/Abbreviation/ Initialization	Description
SOE	Storage Operating Environment
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. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1R2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1R2, September 2007.

d. EMC Corporation EMC® CLARiiON® FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems Security Target, Revision No. 0.5, 12 January 2010.

e. Evaluation Technical Report (ETR) for EAL 2+ Common Criteria Evaluation of EMC Corporation EMC® CLARiiON® FLARE v4.29 with Navisphere v6.29 running on CX4 Series Storage Systems , Common Criteria Evaluation Number: 383-4-120, Document No. 1626-000-D002, Version 1.1, 8 January 2010.