Certification Report

EAL 2+ Evaluation of

EMC CLARiiON® FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-64-CR
Version: 1.0
Date: 25 September 2007
Pagination: i to v, 1 to 11

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 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. 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 (CSE), 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 CSE, 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 (CSE).

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 Standard 17025, General requirements for the accreditation of calibration and testing 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 Electronic Warfare Associates-Canada, Ltd. 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 25 September 2007, 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/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at http://www.commoncriteriaportal.org/

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.
- FLARE and Navisphere are trademarks of EMC Corporation.
- Microsoft, and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries,
- CVE is a trademark of MITRE Corporation,
- Intel and Pentium are registered trademarks of Intel,
- JAVA and Java Runtime Environment (JRE) are registered trademarks of SUN Microsystems, Inc.
- Linux is a registered trademark of Linus Torvalds. Inc.
- Red Hat is a registered trademark of Red Hat, Inc.
- Sun and Solaris are trademarks of Sun Microsystems, Inc. in the United States and other countries,
- UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

TABLE OF CONTENTS

Executive Summary

The EMC CLARiiON® FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems, from EMC Corporation (hereafter referred to as CLARiiON® FLARE v3.24 with Navisphere v6.24), is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

The CLARiiON® FLARE v3.24 with Navisphere v6.24 is a secure, storage management solution. CLARiiON® FLARE v3.24 with Navisphere v6.24 runs the Navisphere software suite, which includes Navisphere Storage-System Initialization Utility, Navisphere Host and Storage Processor (SP) Agents, Navisphere Server Utility, Navisphere Manger, Navisphere Integrator, Navisphere Storage Management Server, and Navisphere Secure Command Line Interpreter (CLI).

Electronic Warfare Associates-Canada, Ltd. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 24 August 2007 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 CLARiiON® FLARE v3.24 with Navisphere v6.24, 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 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation.

CSE, as the CCS Certification Body, declares that the CLARiiON® FLARE v3.24 with Navisphere v6.24 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+ evaluation is the EMC CLARiiON® FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems (hereafter referred to as CLARiiON® FLARE v3.24 with Navisphere v6.24), from EMC Corporation.

2 TOE Description

The CLARiiON® FLARE v3.24 with Navisphere v6.24 is a secure, storage management solution. CLARiiON® FLARE v3.24 with Navisphere v6.24 runs the Navisphere software suite, which includes Navisphere Storage-System Initialization Utility, Navisphere Host and Storage Processor (SP) Agents, Navisphere Server Utility, Navisphere Manger, Navisphere Integrator, Navisphere Storage Management Server, and Navisphere Secure Command Line Interpreter (CLI). Additional detail is found in Section 2 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the CLARiiON® FLARE v3.24 with Navisphere v6.24 is identified in Section 5 of the ST.

4 Security Target

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

Title: EMC Corporation EMC CLARiiON® FLARE v3.24 with Navisphere v6.24 running on CX3 Series Storage Systems Security Target
Version: 1.2
Date: 5 September 2007

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*.

The CLARiiON® FLARE v3.24 with Navisphere v6.24 is:

a. Common Criteria Part 2 conformant; with 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.1 – Basic flaw remediation.

6 Security Policy

The following statements are representative of the Security Policy:

Authentication and Security Management. Users must authenticate to the CLARiiON® FLARE v3.24 with Navisphere v6.24 before being able to perform any TSF-mediated actions. A user authenticating to the CLARiiON® FLARE v3.24 with Navisphere v6.24 must provide a user name and password for a valid user account. The CLARiiON® FLARE v3.24 with Navisphere v6.24 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 allowed to Read and Write to a Logical Unit Number (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 security policy enforcement refer to the CLARiiON® FLARE v3.24 with Navisphere v6.24 Security Target.

7 Assumptions and Clarification of Scope

Consumers of the CLARiiON® FLARE v3.24 with Navisphere v6.24 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 individuals assigned to manage the CLARiiON® FLARE v3.24 with Navisphere v6.24 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 CLARiiON® FLARE v3.24 with Navisphere v6.24 documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The array(s) upon which CLARiiON® FLARE v3.24 with Navisphere v6.24 is installed resides in a physically secure location and only authorized individuals are granted physical access to the host.

For additional information about the CLARiiON® FLARE v3.24 with Navisphere v6.24 security environment, refer to the ST Section 3 - TOE Security Environment.

7.3 Clarification of Scope

The CLARiiON® FLARE v3.24 with Navisphere v6.24 is intended for use by a non-hostile and well-managed user community. CLARiiON® FLARE v3.24 with Navisphere v6.24 relies on the environment to provide it physical and logical protection.

8 Architectural Information

The TOE is composed of software only running on purpose built hardware, both of which are developed by EMC Corporation.

The CLARiiON® FLARE/Navisphere software runs on the EMC CLARiiON® CX3 UltraScale Series of products. The product series consists of a variety of purpose-built appliances providing fault-tolerant storage with no single points of failure. They provide data replication capabilities, with open systems support and connectivity options, including Fibre Channel.

The TOE uses Fibre Channel to connect with application servers. Fibre Channel is a serial data transfer protocol that operates over copper wire or optical fiber. Networking and input/output protocols can be mapped to Fibre Channel constructs, and then encapsulated and transported within Fibre Channel frames. Fibre Channel technology is used in the implementation of storage area networks, or SANs. A SAN is a network linking servers and workstations to disk arrays, tape backup systems, and other storage devices, typically using Fibre Channel Protocol (FCP). The Fibre Channel SAN allows the application servers to issue input/output (I/O) requests to the TOE, which satisfies those requests using the storage areas assigned to the requesting server.

A Storage Processor (SP) has multiple Fibre Channel front-end ports implementing SCSI drivers for connecting to a SAN switch or for a direct connection to a server. Back-end Fibre Channel ports provide connections for a second SP and storage capacity expansion. The appliance also has two Ethernet local area network (LAN) ports. One port is used to access and manage the storage system via Navisphere. The other is a dedicated port for EMC Customer Service use when onsite.

Navisphere is a storage-system management application for configuring, monitoring, and managing CLARiiON® storage systems. It resides on each storage system SP and is

downloaded to the browser when the Storage Management Server software is accessed. Navisphere provides the following basic functionality:

- Discovery and monitoring of CLARiiON storage systems;
- Storage configuration and allocation;
- Status and configuration information display; and
- Event management.

Navisphere can be used to manage a single storage system or a storage domain (a group of storage systems connected by a network). 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; and
- 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 from the local network or remotely (over the Internet, 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 evaluated configuraton for the CLARiiON® FLARE v3.24 with Navisphere v6.24 comprises:

- CLARiiON® FLARE 03.24.010.5.011 with Navisphere® v6.24 running on CX3-10;
- CLARiiON® FLARE 03.24.020.5.011 with Navisphere® v6.24 running on CX3-20;

- CLARiiON® FLARE 03.24.040.5.011 with Navisphere® v6.24 running on CX3-40; and

- CLARiiON® FLARE 03.24.080.5.011 with Navisphere® v6.24 running on CX3-80.

10 Documentation

The EMC Corporation documents provided to the consumer are as follows:

- EMC Navisphere Manager – Administrator's Guide;
- Navisphere Manager – Online Help;
- Planning Your CX3 Storage-System Configuration; and
- CLARiiON CX3 Setup Guide.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the EMC CLARiiON® FLARE v3.24 with Navisphere v6.24, including the following areas:

Configuration management: An analysis of the CLARiiON® FLARE v3.24 with Navisphere v6.24 Configuration Management (CM) system and associated documentation was performed. The evaluators found that the CLARiiON® FLARE v3.24 with Navisphere v6.24 configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the CLARiiON® FLARE v3.24 with Navisphere v6.24 during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the CLARiiON® FLARE v3.24 with Navisphere v6.24 functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the CLARiiON® FLARE v3.24 with Navisphere v6.24 administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators reviewed the flaw remediation procedures used by EMC for the CLARiiON® FLARE v3.24 with Navisphere v6.24. 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 CLARiiON® FLARE v3.24 with Navisphere v6.24 ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the CLARiiON® FLARE v3.24 with Navisphere v6.24 and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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 had 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. Testing focused on:

[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.

- Identification and authentication;
- Security Management; and
- Basic product functionality.

12.3 Independent Penetration Testing

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

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks.

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

12.4 Conduct of Testing

The CLARiiON® FLARE v3.24 with Navisphere v6.24 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the EMC Massachusetts 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.

12.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that the CLARiiON® FLARE v3.24 with Navisphere v6.24 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 complete documentation for the CLARiiON® FLARE v3.24 with Navisphere v6.24 includes a comprehensive Installation and Administration Guide.

The CLARiiON® FLARE v3.24 with Navisphere v6.24 is straightforward to configure, use and integrate into a corporate network.

EMC Corporation Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

EWA-Canada performed separate site visits to review developer processes and to repeat a sample of developer's tests. Although development security was not part of the evaluation, the evaluators observed that the developer was exceptionally conscious of security. The physical, procedural, and personnel security measures meet or exceed the assurance requirements of higher-level CC evaluations. This is reported on in the CC Evaluation Site Visit Report [3].

15 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
CSE	Communications Security Establishment
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FCP	Fibre Channel Protocol
GUI	Graphical User Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LAN	Local Area Network
LUN	Logical Unit Number
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
RAID	Redundant Array Independent/Inexpensive Disks
SAN	Storage Area Network
SCSI	Small Computer System Interface (iSCSI-Internet SCSI)
SOE	Storage Operating Environment
SP	Storage Processor
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

[3] This report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

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 1.0.

b. Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, version 2.3, August 2005.

d. EMC Corporation CLARiiON® FLARE v3.24 with Navisphere v6.24 Security Target, Revision No. 1.2, 05 September 2007.

e. Evaluation Technical Report (ETR) EMC CLARiiON® FLARE v3.24 with Navisphere v6.24, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-64, Document No. 1541-000-D002, Version 1.3, 24 August 2007.