Certification Report

EMC® VMAX™ Series Appliances with HYPERMAX™ OS 5977

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment, 2015

Document number: 383-4-302-CR
Version: 1.0
Date: 30 July 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 30 July 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 trademarks or trademarks:

- EMC is a registered trademark of EMC Corporation; and
- VMAX and HYPERMAX are trademarks of EMC Corporation.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

EMC® VMAX™ Series Appliances with HYPERMAX™ OS 5977 (hereafter referred to as EMC® VMAX™), from EMC Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that EMC® VMAX™ meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

EMC® VMAX™ is a storage solution which provides a physical storage array combined with operating and management software to fulfill an organization's data storage and availability needs. Application servers can use the storage array to store mission-critical data and facilitate the sharing of important files. The TOE can monitor the integrity of stored user data against unintentional corruption, control access to stored user data and storage space, and control access to administrative functions.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 30 July 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 EMC® VMAX™, 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 EMC® VMAX™ 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 EMC® VMAX™ Series Appliances with HYPERMAX™ OS 5977 (hereafter referred to as EMC® VMAX™), from EMC Corporation.

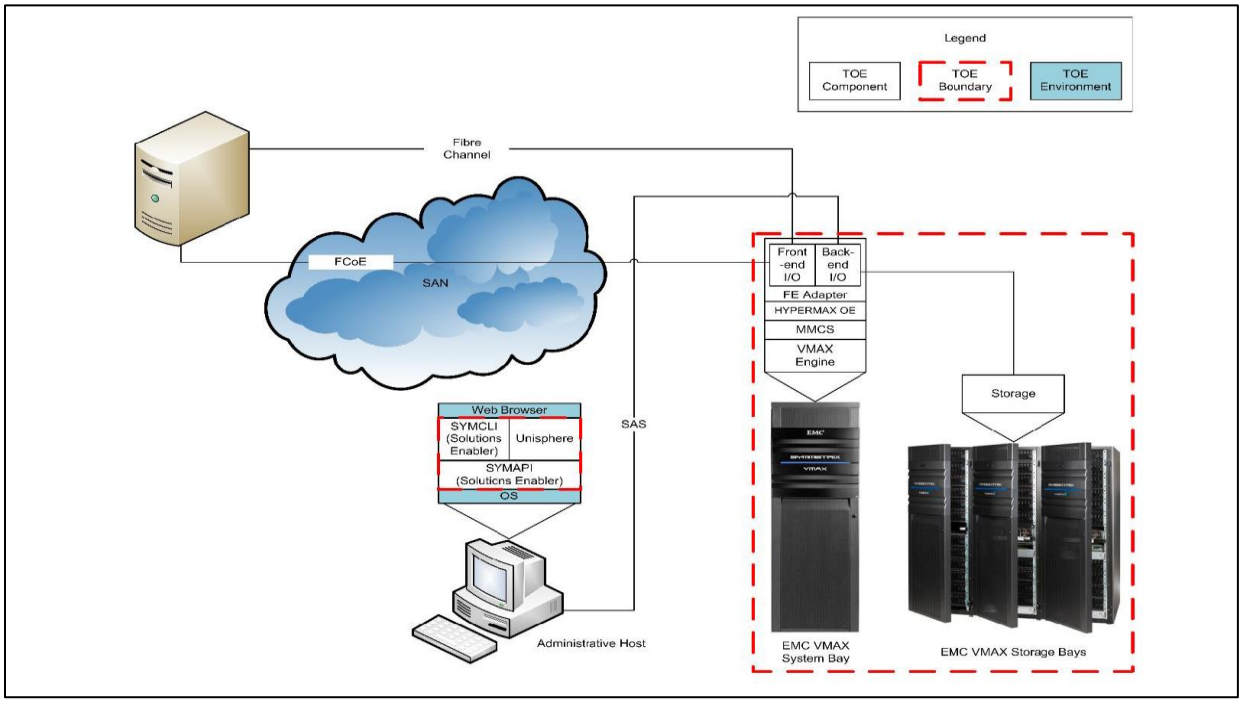
2 TOE Description

EMC® VMAX™ is a storage solution which provides a physical storage array combined with operating and management software to fulfill an organization's data storage and availability needs. Application servers can use the storage array to store mission-critical data and facilitate the sharing of important files. The TOE can monitor the integrity of stored user data against unintentional corruption, control access to stored user data and storage space, and control access to administrative functions.

The TOE includes the VMAX 100K, 200K, and 400K hardware and the following software components:

- HYPERMAX Operating System 5977,
- Solutions Enabler 8.0.2 (Command Line Interface that allows management and
- configuration of VMAX arrays), and
- Unisphere for VMAX 8.0.2 (Web-based Graphical User Interface that allows management and configuration of VMAX arrays).

A diagram of the EMC® VMAX™ architecture is as follows:



3 Security Policy

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

- *Security Audit,*
- *User Data Protection,*
- *Identification and Authentication,*
- *Security Management,*
- *Protection of the TSF, and*
- *TOE Access.*

4 Security Target

The ST associated with this Certification Report is identified below:

EMC® VMAX™ (including VMAX 100K, 200K, and 400K) with HYPERMAX™ OS 5977, Solutions Enabler 8.0.2, and Unisphere for VMAX 8.0.2, Version 2.1, 27 July 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.*

EMC® VMAX™ 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 conformant; with security functional requirements based only upon functional components in Part 2;

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 EMC® VMAX™ 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:

- *There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.*
- *Administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.*
- *KVM or Ethernet connections will not be made to the Management Module Control Station after deployment of the TOE.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The IT Environment will be configured in such a way as to allow TOE users to access the information stored on the TOE.*
- *The IT Environment must block all traffic originating from outside of the controlled access facility intended for the Solutions Enabler ports of the TOE.*
- *The TOE is located within a controlled access facility and is physically available to authorized administrators only.*

7 Evaluated Configuration

The evaluated configuration for EMC® VMAX™ comprises:

- *the VMAX 100K, 200K, and 400K in a Single Engine System Bay Rack configuration, which includes one Engine and two Disk Array Enclosures*
- *the HYPERMAX OS 5977 installed on the VMAX hardware*
- *Solutions Enabler 8.0.2 and Unisphere for VMAX 8.0.2 installed on the administrative host*

The requirements for the TOE environment include:

- *an administrative host with Windows Server 2012 R2 and Internet Explorer 11 installed on general purpose hardware*
- *a server with a Host Bus Adapter connected to the Storage Area Network, running Windows Server 2012 R2 installed on general purpose hardware*

The publication entitled EMC Corporation EMC® VMAX™ (including VMAX 100K, 200K, and 400K) with HYPERMAX™ OS 5977, Solutions Enabler 8.0.2, and Unisphere for VMAX 8.0.2 Guidance Documentation Supplement v0.7, July 27, 2015 describes the procedures necessary to install and operate EMC® VMAX™ in its evaluated configuration.

8 Documentation

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

a. EMC® VMAX Family with HYPERMAX OS Product Guide, June 2015;

b. EMC® VMAX Family 100K, 200K, and 400K Planning Guide, June 2015;

c. EMC® VMAX Family Security Configuration Guide, March 2015;

d. EMC® VMAX Family with HPERMAX OS 5977 Release Level HYPERMAX OS 5977.596.583 Release Notes, April 2012;

e. EMC® Solutions Enabler Array Management CLI User Guide Version 8.0.2, March 2015;

f. EMC® Solutions Enabler SRM Version 8.0.2 CLI User Guide, March 2015;

g. EMC® Solutions Enabler CLI Version 8.0.2 Command Reference, March 2015;

h. EMC® Solutions Enabler, VSS Provider, and SMI-S Provider Version 8.0.2 Release Notes, May 2015;

i. EMC® Unisphere for VMAX Version 8.0.2 Release Notes, April 2015;

j. EMC® Solutions Enabler Version 8.0.2 Installation Guide, April 2015 ;

k. EMC Corporation EMC® VMAX™ (including VMAX 100K, 200K, and 400K) with HYPERMAX™ OS 5977, Solutions Enabler 8.0.2, and Unisphere for VMAX 8.0.2 Guidance Documentation Supplement v0.7, July 27, 2015 ; and

l. EMC® Unisphere for VMAX Version 8.0.2 Installation Guide, June 2015.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of EMC® VMAX™, including the following areas:

Development: The evaluators analyzed the EMC® VMAX™ 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 EMC® VMAX™ 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 EMC® VMAX™ 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 EMC® VMAX™ configuration management system and associated documentation was performed. The evaluators found that the EMC® VMAX™ 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 EMC® VMAX™ during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the EMC® VMAX™. 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;

b. Block Storage Access Control Review: The objective of this test goal is to examine and confirm the rules claimed for the Block Storage Access Control Policy:

c. De-allocation: The objective of this test goal is to confirm that the previous information content of a resource is made unavailable upon removal of the disk from the storage array;

d. RAID 5: The objective of this test goal is to confirm that the TOE supports RAID 5;

e. Unisphere and Roles: The objective of this test goal is to confirm that role enforcement is performed on the Unisphere interface; and

f. Solutions Enabler and Roles: The objective of this test goal is to confirm that role enforcement is performed on the Solutions Enabler interface.

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.

[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.

b. Functionality available prior to login: The objective of this test goal is to attempt to access sensitive information prior to login.

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

10.4 Conduct of Testing

EMC® VMAX™ was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. 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 EMC® VMAX™ 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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FCoE	Fibre Channel over Ethernet
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories - Canada
SAS	Serially Attached SCSI
SCSI	Small Computer System Interface
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. EMC® VMAX™ (including VMAX 100K, 200K, and 400K) with HYPERMAX™ OS 5977, Solutions Enabler 8.0.2, and Unisphere for VMAX 8.0.2, Version 2.1, 27 July 2015.

e. Evaluation Technical Report for EMC® VMAX™ (including VMAX 100K, 200K, and 400K) with HYPERMAX™ OS 5977, Solutions Enabler 8.0.2, and Unisphere for VMAX 8.0.2 Document No. 1852-000-D002, Version 0.3, 30 July 2015.