Certification Report

EAL 2+ Evaluation of EMC VPLEX with GeoSynchrony version 5.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-200-CR
Version: 1.0
Date: 9 January 2012
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, 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, 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 9 January 2012, 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:

- GeoSynchrony® is a registered trademark of EMC Corporation.

- VPLEX™ is a trademark of EMC Corporation.

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

TABLE OF CONTENTS

Executive Summary

EMC VPLEX with GeoSynchrony version 5.0 (hereafter referred to as VPLEX), from EMC Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

VPLEX is a storage network-based federation solution that provides non-disruptive, heterogeneous data movement and volume management functionality. VPLEX is a software-only TOE that connects to a fibre channel (FC) storage area network (SAN) or to Ethernet switches. The VPLEX architecture is designed as a high availability solution.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 9 December 2011 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 VPLEX, 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 VPLEX 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 VPLEX with GeoSynchrony version 5.0 (hereafter referred to as VPLEX), from EMC Corporation.

2   TOE Description

VPLEX is a storage network-based federation solution that provides non-disruptive, heterogeneous data movement and volume management functionality. VPLEX is a software-only TOE that connects to a Fibre Channel (FC) Storage Area Network (SAN) or Ethernet switches. The TOE enforces an access control policy on hosts attempting to read from or write to the storage that the TOE controls. The VPLEX architecture is designed as a high availability solution.

The TOE consists of only the software portion of VPLEX, which is comprised of the following:

- The management server software, including the VPLEX command line interface (CLI) and the management console web-based graphical user interface (GUI). The management server software is used to issue administrative commands;
- The director software which facilitates Input/Output communication between the front-end hosts and the back-end storage arrays in a SAN; and
- The VPLEX witness software which provides availability and integrity protection for data controlled by the TOE.

The Metro deployment configuration (synchronous communications between two or more clusters) and the Geo deployment configuration (asynchronous communications between two or more clusters) are the two evaluated configurations.

3   Evaluated Security Functionality

The complete list of evaluated security functionality for VPLEX is identified in Sections 5 and 6 of the ST.

4   Security Target

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

Title: EMC Corporation VPLEX with GeoSynchrony 5.0 Security Target
Version: 0.6
Date: 6 December 2011

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*.

VPLEX is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST:

   • EXT_FPT_RTC.1 - Replicated TSF Data Consistency;

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

VPLEX implements a Storage Access Control policy that controls host access to storage based on security attributes. Details of this security policy can be found in Section 6 of the ST.

In addition, VPLEX implements policies pertaining to security audit, user data protection, identification and authentication, security management, protection of the TOE Security Functionality (TSF) and TOE access. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of VPLEX 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:

- It is assumed there are one or more competent individuals assigned to manage the TOE and they are properly trained, follow all guidance, and are non-hostile.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is located in a controlled access facility and available only to authorized administrators.

- It is assumed the TOE will be implemented in a SAN environment that is securely configured and can obtain reliable timestamps.

- It is assumed that the IT Environment will be configured in such a way as to allow TOE users to access the information stored on the TOE.

- It is assumed that remote session connections are secured by the IT environment.

7.3 Clarification of Scope

The TOE environment must be properly configured with front-end switches and back-end storage area networks for host machines to securely communicate with storage.

8 Evaluated Configuration

The evaluated configuration for VPLEX comprises:

a. The management server software and director software with GeoSynchrony version 5.0.0.00.00.38 operating on a custom designed VPLEX appliance.

b. The VPLEX Witness software version 5.0.0.00.00.38 operating on VMware ESX v4.1.

The publication entitled VPLEX with GeoSynchrony™ 5.0 Guidance Documentation Supplement version 0.1 describes the procedures necessary to install and operate VPLEX in its evaluated configuration.

9 Documentation

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

a. EMC® VPLEX™ Getting Started Guide version A03;

b. EMC® VPLEX™ with GeoSynchrony™ 5.0 Product Guide version A01;

c. Implementation and Planning Best Practices for EMC® VPLEX™ Technical Notes version 5.0;

d. EMC® VPLEX™ with GeoSynchrony™ 5.0.1 Release Notes version A02;

e. EMC® VPLEX™ with GeoSynchrony™ 5.0 Configuration Guide version A05;

f. EMC® VPLEX™ Hardware Installation Guide version 5.0;

g. EMC® VPLEX™ with GeoSynchrony™5.0 CLI Guide version A01;

h. EMC® VPLEX™ Security Configuration Guide version A05;

i. EMC® VPLEX™ with GeoSynchrony™ 5.0 Management Console Help (online help); and

j. EMC® VPLEX™ with GeoSynchrony™ 5.0 Best Practices Guide version 5.0.

10 Evaluation Analysis Activities

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

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

The evaluators reviewed the flaw remediation procedures used by the developer for VPLEX. 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 VPLEX. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify VPLEX potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the VPLEX in its operational environment.

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

11 ITS Product Testing

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

11.1 Assessment of Developer Tests

The evaluators verified that the developers have 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.

11.2 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 is the following list of EWA-Canada test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests and provide coverage for most of the TOE Security Functions;

b. User Data Protection: The objective of this test goal is to verify that TOE users will be granted access only to user data for which they have been authorized; and

c. Identification and Authentication: The objective of this test goal is to verify the TOE password strength policy is being implemented.

---

[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.

11.3 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. Search of public domain security sites to determine if there are any known or potential vulnerabilities that could be exploited;

b. Direct Attacks to verify that the TOE web interface does not divulge any proprietary information and cannot be bypassed to access other resources;

c. Verification that user login credential requirements cannot be bypassed; and

d. Verification that an administrative user of the TOE cannot gain root level access to the underlying operating system of the TOE.

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

11.4 Conduct of Testing

VPLEX was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the developer testing facility located in Hopkinton, Massachusetts. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

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

12 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.

13 Evaluator Comments, Observations and Recommendations

The complete documentation set for the TOE includes a comprehensive Installation and Security Guide and Users Guide.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/   Description
Initialization

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FC	Fibre Channel
GUI	Graphical User Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LAN	Local Area Network
PALCAN	Program for the Accreditation of Laboratories – Canada
SAN	Storage Area Network
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
WAN	Wide Area Network

15 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 3, July 2009.

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

d.   EMC Corporation VPLEX with GeoSynchrony 5.0 Security Target, version 0.6, 6 December 2011.

e.   Evaluation Technical Report for EAL2+ Common Criteria Evaluation of EMC Corporation VPLEX with GeoSynchrony 5.0, Version 1.0, 9 December 2011.