Certification Report

EMC® ProSphere™ v2.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-237-CR
Version:	1.0
Date:	26 June 2013
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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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.

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 26 June 2013, 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 trademarks or registered trademarks:

- EMC is a registered trademark of EMC Corporation; and
- ProSphere 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® ProSphere™ v2.0 (hereafter referred to as ProSphere), from EMC Corporation Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

ProSphere gives an enterprise-level view of an organization's data center. It enables administrators to discover, monitor, and report on all storage-related resources across the data center from a single workstation. ProSphere also allows administrators to monitor capacity utilization of the environment, measure application performance, and be notified of conditions that require attention, such as performance thresholds. ProSphere is deployed as a collection of interdependent virtual machines (VM) configured at the VM and virtual application (vApp) level.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 21 May 2013 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 ProSphere, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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: e.g. ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the ProSphere 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® ProSphere™ v2.0 (hereafter referred to as ProSphere), from EMC Corporation

2 TOE Description

ProSphere gives an enterprise-level view of an organization's data center. It enables administrators to discover, monitor, and report on all storage-related resources across the data center from a single workstation. ProSphere also allows administrators to monitor capacity utilization of the environment, measure application performance, and be notified of conditions that require attention, such as performance thresholds. ProSphere is deployed as a collection of interdependent virtual machines (VM) configured at the VM and virtual application (vApp) level.

A detailed description of the ProSphere architecture is found in Section 1.4 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for ProSphere is identified in Section 6 of the ST.

4 Security Target

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

Title: EMC® ProSphere™ v2.0 Security Target
Version: 0.7
Date: 1 May 2013

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.*

ProSphere 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

ProSphere implements an access control policy to control user access to the system; details of this security policy can be found in Section 6 of the ST.

In addition, ProSphere implements policies pertaining to security audit, user data protection, identification and authentication, Protection of the TOE and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions

Consumers of ProSphere 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:

- Administrators are non-hostile, appropriately trained, and follow all administrative guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is located within a controlled access facility; and
- The TOE is installed on the appropriate hypervisor and hardware.

8 Evaluated Configuration

The evaluated configuration for the ProSphere software only TOE comprises:

- a GPC with VMware ESXI Server running the following software:
    - ProSphere Application v2.0.0.0.271
    - Discovery Engine v3.1.0.0.265

  - Historical Database v2.0.0.0.254

- a GPC with VMware ESXI Server running the following software:
  - Discovery Engine Collector v3.1.0.0.265

The following publications entitled EMC ProSphere v2.0 Administrators Guide, EMC ProSphere v2.0 Deployment Guide, EMC ProSphere v2.0 Security Configuration Guide and EMC ProSphere v2.0 Guidance Documentation Supplement describes the procedures necessary to install and operate ProSphere in its evaluated configuration.

9 Documentation

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

a. EMC ProSphere v2.0 Administrators Guide, April, 2013;
b. EMC ProSphere v2.0 Deployment Guide April, 2013;
c. EMC ProSphere v2.0 Release Notes April 26, 2013;
d. EMC ProSphere v2.0 Security Configuration Guide April, 2013;
e. EMC ProSphere v2.0 RestAPI April 2013; and
f. EMC ProSphere v2.0 Guidance Documentation Supplement, v0.1, 1 May 2013.

10 Evaluation Analysis Activities

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

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

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

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

11 ITS Product Testing

Testing 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 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.

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.

[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.

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;

b. TLS 1.0 or higher: The objective of this test case is to confirm that ProSphere supports TLS 1.0;

c. LDAP for login: The objective of this test goal is to confirm that ProSphere uses LDAP to authenticate a user;

d. Security Compliance Message: The objective of this test goal is to confirm that the login banner can be created and edited and requires users to acknowledge it before accessing Proshere; and

e. Verify Secure Communications: The objective of this test goal is to confirm that communications between TOE components is not in the clear.

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. Port Scan: The objective of this test goal is to scan the TOE using a port scanner to reveal any potential avenues of attack;

b. Tool Scanning: The objective of this test goal is to scan the TOE for known and unknown weaknesses relevant to TOE type;

c. Misuse: the objective of this test goal is to perform an administrative action that could render the system vulnerable; and

d. Multiple Administrative Sessions: The objective of this test goal is to confirm that the TOE supports multiple Security Administrator sessions and that the last change made is what is saved and retained.

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

11.4 Conduct of Testing

ProSphere was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place on site at the EMC QA facility in Hopkinton, MA, as the required operational environment is not supported in the EWA

Information Technology Security Evaluation and Testing Facility (ITSET). 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 ProSphere 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 developer maintains a complete set of user guidance including security configuration recommendations. The developer also performs regular security assessments and scans of the TOE in order to maintain security.

14 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
GPC	General Purpose Computer
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LDAP	Lightweight Directory Access Protocol
PALCAN	Program for the Accreditation of Laboratories - Canada
QA	Quality Assurance
SFR	Security Functional Requirement
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation

Acronym/Abbreviation/ Initialization	Description
vApp	Virtual Application
VM	Virtual Machine

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® ProSphere™ v2.0 Security target, v0.7, 1 May 2013.

e. ETR for EAL 2+ EMC® ProSphere™ v2.0, version 1.3, 21 May 2013.