Certification Report

EAL 2+ Evaluation of EMC RecoverPoint version 3.4

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-159-CR
Version:	1.0
Date:	10 June 2011
Pagination:	i to iii, 1 to 7

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, 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 10 June 2011, and the security target identified in Section 4 of this report.

This certification report makes reference to the following trademarks and registered trademarks:

- Linux is a registered trademark of Linus Torvalds Inc.; and
- Dell, PowerEdge are trademarks of Dell Incorporated.

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

TABLE OF CONTENTS

Executive Summary

EMC RecoverPoint version 3.4 (hereafter referred to as EMC RecoverPoint), from EMC Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

EMC RecoverPoint is a software product that runs on RecoverPoint appliances (RPAs), providing real-time data replication for systems and devices in an enterprise storage area network (SAN) environment.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 5 May 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 EMC RecoverPoint, 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 EMC RecoverPoint 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 Evaluation Assurance Level (EAL) 2 augmented evaluation is EMC RecoverPoint version 3.4 (hereafter referred to as EMC RecoverPoint), from EMC.

[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.

2 TOE Description

EMC RecoverPoint is a software product that runs on RecoverPoint appliances (RPAs), providing real-time data replication functionality for systems and devices in an enterprise storage area network (SAN) environment.

Data replication is enabled by components identified as splitters (not included in the evaluation) that simultaneously direct application writes to both normally designated storage and to the RPA.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the EMC RecoverPoint version 3.4 is identified in Sections 5 and 6 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 RecoverPoint version 3.4 Security Target
Version: 0.6
Date: 23 March 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*.

The EMC RecoverPoint is:

a. *Common Criteria Part 2 extended*, with functional requirements based on functional components in Part 2, except for the following explicitly stated requirement defined in the ST: EXT_FDP_ITT.1 - Basic recovery transfer protection.

b. *Common Criteria Part 3 conformant*, with security assurance requirements based on assurance components in Part 3; and

c. *Common Criteria EAL 2 augmented*, containing all the security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 - Flaw Reporting Procedures.

6 Security Policy

EMC RecoverPoint enforces: a Replication Access Control Policy on volumes [2]; a Group Access Control Policy on volumes and splitters; and an Information Flow Control Policy on data exchanged between RPAs.

In addition, EMC RecoverPoint implements policies pertaining to security audit, user data protection, identification and authentication, security management, protection of the TSF, and TOE access.

[2] Refer ST Section 7.1.2 User Data Protection for additional detail on volumes.

Further details on these security policies may be found in Sections 5 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of EMC RecoverPoint 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:

a. There are one or more competent individuals assigned to manage the TOE and the security of the information it contains; and

b. The TOE will be managed by competent individuals that are non-hostile, appropriately trained, and follow all guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

a. All ports required for communication between local and remote TOE installations are open, and the TOE is protected from all other traffic outside the controlled access facility where the TOE is housed;

b. The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access;

c. The TOE will be placed in a network infrastructure such that host information to be replicated and restored will always maintain connection to the TOE; and

d. The TOE will be placed in a SAN which contains sufficient Logical Unit Number (LUN) masking and port zoning to not allow unrelated hosts access to RecoverPoint owned LUNs.

8 Evaluated Configuration

RecoverPoint version 3.4 is a software TOE that includes a customized Linux Kernel 2.6.32.9.

EMC RecoverPoint supports three replication configurations: Continuous Data Protection (CDP), Continuous Remote Replication (CRR) and Concurrent Local and Remote (CLR). In a CDP configuration, a local SAN connects to a local RPA for local replication. CDP is designed to allow operational recovery from logical corruptions such as human errors or viruses. In a CRR configuration, two geographically separated SANs are connected by two RPA clusters for remote replication. CRR is designed to allow recovery primarily from geographical or site disasters. The CLR configuration combines CDP and CRR replication functionality.

The TOE runs on the Dell PowerEdge 1950 phase 3 (Gen3), Dell PowerEdge 2950 phase 3, and Dell PowerEdge R610 (Gen4) RecoverPoint appliances (RPAs).

The publication entitled RecoverPoint version 3.4 Security Configuration Guide describes the procedures necessary to install and operate EMC RecoverPoint in its evaluated configuration.

9 Documentation

The EMC documents provided to the consumer are as follows:

a. RecoverPoint version 3.4 Administrator's Guide;

b. RecoverPoint version 3.4 Deployment Manager Product Guide;

c. RecoverPoint version 3.4 Installation Guide;

d. RecoverPoint version 3.4 Security Configuration Guide; and

e. RecoverPoint version 3.4 CLI Reference Guide.

10 Evaluation Analysis Activities

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

Development: The evaluators analyzed the EMC RecoverPoint 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 RecoverPoint security architectural description and determined that the initialization process is secure and 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 RecoverPoint 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 RecoverPoint configuration management system and associated documentation was performed. The evaluators found that the EMC RecoverPoint 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 EMC RecoverPoint during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used for EMC RecoverPoint. 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 EMC RecoverPoint. Additionally, the evaluators conducted a review of public domain vulnerability databases. The evaluators did not identify any potential vulnerabilities applicable to the EMC RecoverPoint 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 developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[3].

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 the developer's test cases, and creating test cases that augmented the developer tests.

For this evaluation, the TOE was tested at EMC development location in Tel Aviv Israel. All evaluator 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. Initialization: The objective of this test goal is to confirm that the TOE is installed and configured into the evaluated configuration;

b. Repeat of Developer's Tests: The objective of this test goal is to repeat the complete set of the developer's tests; and

c. Authentication and AlertsTests: The objective of this test goal is to exercise the TOE's authentication and email alerts functionality.

[3] 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 comprising port scanning.

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

11.4 Conduct of Testing

EMC RecoverPoint was subjected to formally documented, independent functional and penetration tests. The testing took place at the EMC development location in Tel Aviv, Israel. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Procedures and Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that EMC RecoverPoint behaves as specified in its ST, functional specification, TOE design, and security architecture description.

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 documentation for the EMC RecoverPoint includes a comprehensive Installation, Administration, and Security Configuration Guide.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CDP	Continuous Data Protection
CLR	Concurrent Local and Remote Replication
CLI	Command Line Interface
CPL	Certified Products list
CRR	Continuous Remote Replication
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology

Acronym/Abbreviation/ Initialization	Description
ITSET	Information Technology Security Evaluation and Testing
LUN	Logical Unit Number
PALCAN	Program for the Accreditation of Laboratories Canada
RPA	RecoverPoint appliance
SAN	Storage Area Network
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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 EMC RecoverPoint version 3.4 Security Target, Version 0.6, 23 March 2011.

e. Evaluation Technical Report (ETR) EMC RecoverPoint version 3.4, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-159, Document No. 1669-000-D002, Version 1.1, 5 May 2010.