Certification Report

EAL 2+ Evaluation of

Data Domain® Operating System Version 5.2.1.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-233-CR
Version: 1.0
Date: 08 May 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 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 17 May 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 and Data Domain are registered trademarks of EMC Corporation.

TABLE OF CONTENTS

Executive Summary

Data Domain® Operating System Version 5.2.1.0 (hereafter referred to as DDOS 5.2.1.0), from EMC Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

DDOS 5.2.1.0 is a disk-based deduplication software storage operating system, which stores only unique segments of files on disk. The software TOE runs on a series of appliances supplied by EMC®, which differ in storage and throughput capacity. DDOS 5.2.1.0 is managed via a Command Line Interface (CLI) at the console of the local system or via a web-based Graphical User Interface (GUI) hosted on the local system and accessed over a network connection from a management workstation. Administrators use a secure connection to connect to both interfaces.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 25 April 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 DDOS 5.2.1.0, 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 DDOS 5.2.1.0 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 Data Domain® Operating System Version 5.2.1.0 (hereafter referred to as DDOS 5.2.1.0), from EMC Corporation.

2 TOE Description

DDOS 5.2.1.0 is a disk-based deduplication software storage operating system, which stores only unique segments of files on disk. The software TOE runs on a series of appliances supplied by EMC®, which differ in storage and throughput capacity. DDOS 5.2.1.0 is managed via a Command Line Interface (CLI) at the console of the local system or via a web-based Graphical User Interface (GUI) hosted on the local system and accessed over a network connection from a management workstation. Administrators use a secure connection to connect to both interfaces.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for DDOS 5.2.1.0 is identified in Section 6 of the ST.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in DDOS 5.2.1.0:

Cryptographic Algorithm	**Standard**	**Certificate #**
Symmetric encryption and decryption	FIPS 197	810
Random Number Generator	SB-800-90	2

4 Security Target

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

Title: EMC Corporation Data Domain® Operating System Version 5.2.1.0
Version: 0.11
Date: 18 March 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.*

DDOS 5.2.1.0 is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - EXT_FDD_DDR.1 - Duplicate Data Removal;
   - EXT_FRU_RLP.1 - Minimum and Maximum retention lock periods; and
   - EXT_FPT_TRC.1 - Internal 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: e.g. ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

DDOS 5.2.1.0 implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information to and from the system; details of these security policies can be found in Section 6 of the ST.

In addition, DDOS 5.2.1.0 implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of DDOS 5.2.1.0 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 are one or more competent individuals assigned to manage the TOE and the security of the information it contains; and
- Administrators are non-hostile, appropriately trained, and follow all administrative guidance.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- Physical security will be provided for the TOE and its environment.

7.3 Clarification of Scope

DDOS 5.2.1.0 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. DDOS 5.2.1.0 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

DDOS 5.2.1.0 incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

8 Evaluated Configuration

The evaluated configuration for DDOS 5.2.1.0 comprises the Data Domain Operating System version 5.2.1.0 software application build number 331816 running on the following DDOS appliances: DD120, DD140, DD160, DD510, DD530, DD565, DD580, DD580G, DD610, DD620, DD 630, DD640,DD660, DD670, DD690, DD690G, DD860, DDARCHIVER860, DD880, DD880G, DD880GDA, DD890, DD890GDA, DD990.

The publication entitled EMC Data Domain Operation System Initial Configuration Guide version 5.2 describes the procedures necessary to install and operate DDOS 5.2.1.0 in its evaluated configuration.

9 Documentation

The EMC documents provided to the consumer are as follows:

a. EMC® Data Domain Operating System Release Notes Version 5.2
b. EMC® Data Domain Operating System Initial Configuration Guide Version 5.2
c. EMC® Data Domain Operating System Command Reference Guide Version 5.2
d. EMC® Data Domain Operating System Administration Guide Version 5.2

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of DDOS 5.2.1.0, including the following areas:

Development: The evaluators analyzed the DDOS 5.2.1.0 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 DDOS 5.2.1.0 security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the DDOS 5.2.1.0 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 DDOS 5.2.1.0 configuration management system and associated documentation was performed. The evaluators found that the DDOS 5.2.1.0 configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well-developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the DDOS 5.2.1.0 design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of DDOS 5.2.1.0 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Data Domain for DDOS 5.2.1.0. During a site visit, the evaluators 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 DDOS 5.2.1.0. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to DDOS 5.2.1.0 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[2].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design 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;

b. Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration as identified in ST;

c. Security Management: The objective of this test goal is to exercise the Management functions by creating accounts, role assignment, and account deletion, using both the GUI and CLI interfaces when possible;

d. Identification and Authentication: The objective of this test goal is to confirm the identification and authentication requirements have been met; and

e. Audit: The objective of this test goal is to confirm the audit requirements have been met.

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:

[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.

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; and

c. Information Leakage Verification: The objective of this test goal is to monitor for leakage during start-up, shutdown, login and other scenarios where subsystems are communicating with each other.

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

11.4 Conduct of Testing

DDOS 5.2.1.0 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at EWA-Canada. 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.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that DDOS 5.2.1.0 behaves as specified in its ST and functional specification and TOE design.

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 evaluator recommends that the users read the ST and make sure all the assumptions made regarding the environment are true in the intended environment of the TOE. The TOE must be installed within a non-hostile and well-managed operating environment.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility

Acronym/Abbreviation/ Initialization	Description
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
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 Data Domain® Operating System version 5.2.1.0 Security Target v0.11, 18 March 2013.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of EMC Corporation EMC® Data Domain® Operating System Version 5.2.1.0, v1.1, 25 April 2013.