Certification Report

EMC Isilon® OneFS® v7.2.0.4

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-338-CR
Version: 1.0
Date: 14 December 2015
Pagination: i to iii, 1 to 11

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 14 December 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).

TABLE OF CONTENTS

Executive Summary

EMC Isilon® OneFS® v7.2.0.4 from EMC Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that EMC Isilon® v7.2.0.4 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

EMC Isilon® OneFS® v7.2.0.4 combines the three layers of storage architecture—file system, volume manager, and data protection – into a scale-out NAS cluster. Each node adds resources to the cluster. Because each node contains globally coherent RAM, as a cluster becomes larger, it becomes faster. Meanwhile, the file system expands dynamically and redistributes content, which eliminates the work of partitioning disks and creating volumes. Segmenting and distributing data —a process known as striping—not only protects data, but also enables a user connecting to any node to take advantage of the entire cluster's performance.

The TOE uses distributed software to scale data across commodity hardware. Nodes work as peers to spread data across the cluster. No master device controls the cluster; no slaves invoke dependencies. Instead, each node helps control data requests, boosts performance, and expands the cluster's capacity.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 14 December 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 Isilon® v7.2.0.4, 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 Isilon® v7.2.0.4 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

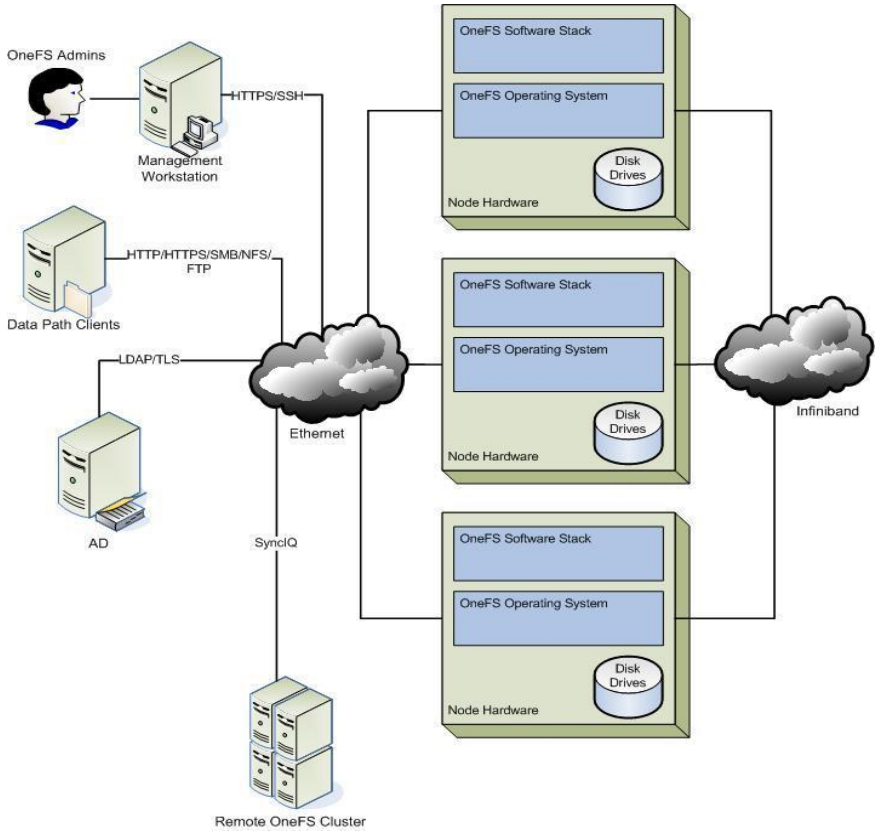
The Target of Evaluation (TOE) for this EAL 2+ evaluation is EMC Isilon® OneFS® v7.2.0.4 from EMC Corporation.

2 TOE Description

EMC Isilon® OneFS® v7.2.0.4 combines the three layers of storage architecture—file system, volume manager, and data protection – into a scale-out NAS cluster. Each node adds resources to the cluster. Because each node contains globally coherent RAM, as a cluster becomes larger, it becomes faster. Meanwhile, the file system expands dynamically and redistributes content, which eliminates the work of partitioning disks and creating volumes. Segmenting and distributing data —a process known as striping—not only protects data, but also enables a user connecting to any node to take advantage of the entire cluster's performance.

The TOE uses distributed software to scale data across commodity hardware. Nodes work as peers to spread data across the cluster. No master device controls the cluster; no slaves invoke dependencies. Instead, each node helps control data requests, boosts performance, and expands the cluster's capacity.

A diagram of the EMC Isilon® OneFS® v7.2.0.4 architecture is as follows:



3 Security Policy

EMC Isilon® OneFS® v7.2.0.4 implements a role-based access control policy to control administrative access to the system. In addition, EMC Isilon® OneFS® v7.2.0.4 implements policies pertaining to the following security functional classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of TOE Security Functions
- Resource Utilization
- TOE Access

4 Security Target

The ST associated with this Certification Report is identified below:

EMC Corporation Isilon® OneFS® v7.2.0.4 Security Target, Document Version 1.0, December 3, 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 Isilon® v7.2.0.4 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 Isilon® OneFS® v7.2.0.4 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:

- *The TOE software will be protected from unauthorized modification.*
- *There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.*

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- *The TOE is located within a controlled access facility.*

7 Evaluated Configuration

The evaluated configuration for EMC Isilon® OneFS® v7.2.0.4 comprises:

The TOE firmware (EMC Isilon® OneFS® v7.2.0.4 with patch 164118) installed on one of the following TOE hardware platforms:

- S210
- X410
- NL400
- HD400

With the following environmental components:

- S210
  - Arista 7150S (front-end)
  - Flextronics F-X430044 (back-end)
- X410
  - Arista 7150S (front-end)
  - Intel Qlogic 12000 (back-end)
- NL400
  - Intel Qlogic 12200
- HD400
  - Cisco Catalyst 3750, Brocade VDX6740 (front end)
  - Mellanox IS5023 (back-end)

Client systems (the following were used in the evaluated configuration):

- Microsoft Windows 8
- Red Hat Enterprise Linux 5

Active Directory domain controller (Windows Server 2008 R2)

The publication entitled Isilon OneFS v7.2 Guidance Documentation Supplement, Document Version 0.5, December 3, 2015 describes the procedures necessary to install and operate EMC Isilon® v7.2.0.4 in its evaluated configuration.

8 Documentation

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

a. Isilon OneFS API Reference, Version 7.2, March 2015
b. Isilon OneFS Backup and Recovery Guide, Version 7.2, March 2015
c. Isilon OneFS CLI Administration Guide, Version 7.2, March 2015
d. Isilon Supportability & Compatability Guide, June 17, 2015
e. Isilon OneFS Version 7.2 Event Reference, Version 7.2, March 2015
f. HD400 Installation Guide, June 2015
g. Isilon OneFS Migration Tools Guide, Version 7.2, March 2015
h. NL400 Instalation Guide, REV H, June 2015
i. Isilon OneFS Release Notes, 7.2.0, March 2015
j. OneFS RESTful Access to the Namespace API Reference, October 2013
k. S210 Installation Guide, June 2015
l. Isilon OneFS Security Configuration Guide, Version 7.2, March 2015
m. Isilon Site Preparation and Planning Guide, July 2015
n. Isilon OneFS Web Administration Guide, Version 7.2, March 2015; and
o. X410 Installation Guide, June 2015.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of EMC Isilon® OneFS® v7.2.0.4, including the following areas:

Development: The evaluators analyzed the EMC Isilon® OneFS® v7.2.0.4 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 Isilon® OneFS® v7.2.0.4 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 Isilon® OneFS® v7.2.0.4 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 Isilon® OneFS® v7.2.0.4 configuration management system and associated documentation was performed. The evaluators found that the EMC Isilon® OneFS® v7.2.0.4 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 Isilon® OneFS® v7.2.0.4 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the EMC Isilon® OneFS® v7.2.0.4. 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. Front panel functionality: The objective of this test goal is to determine what functionality is available to users of the front panel;

c. Unauthenticated Functionality: The objective of this test goal is to confirm what functionality is available to unauthenticated users;

d. Auditing: The objective of this test goal is to confirm the auditing capability of the TOE; and

e. Roles: The objective of this test goal is to confirm the permissions available to each role.

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; and

b. OpenSSH MaxAuthTries Exploit: This test attempts to use the OpenSSH MaxAuthTries exploit that was uncovered during the vulnerability scan.

[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.

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

10.4 Conduct of Testing

EMC Isilon® OneFS® v7.2.0.4 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 Isilon® OneFS® v7.2.0.4 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
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NAS	Network Attached Storage
PALCAN	Program for the Accreditation of Laboratories - Canada
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 Corporation Isilon® OneFS® v7.2.0.4 Security Target, Document Version 1.0, December 3, 2015

e. ETR for EAL 2+ CC Evaluation of Isilon® OneFS® v7.2.0.4, v0.4, December 14, 2015.