Certification Report

EAL 2+ Evaluation of EMC Isilon® OneFS® v6.5.4

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-204-CR
Version: 1.0
Date: 18 April 2012
Pagination: i to iii, 1 to 9

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 April 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 trademarks or registered trademarks:

- Isilon®, SyncIQ® and OneFS® are registered trademarks of EMC Corporation.
- FlexProtect™, SmartConnect™, SnapshotIQ™, and SmartPools™ are trademarks of EMC Corporation

TABLE OF CONTENTS

Executive Summary

EMC Isilon® OneFS® v6.5.4 (hereafter referred to as OneFS), from EMC Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

OneFS is a software-only TOE. It is an operating system that provides distributed file system management, and is made up of the following software components; OneFS ® v6.5.4 , FlexProtect™, SmartConnect™ Advanced, SyncIQ ® , SmartQuotas, SnapshotIQ™ , SmartPools™, and iSCSI

Authenticated administrators can manage the TOE through either the CLI or the Web Administration GUI. Users access the file system through a front end Local Area Network and must authenticate prior to access.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed in April 2012 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 OneFS, 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 OneFS 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 Isilon® OneFS® v6.5.4 (hereafter referred to as OneFS), from EMC Corporation.

2 TOE Description

OneFS is a software-only TOE. It is an operating system that provides distributed file system management, and is made up of the following software components:

- OneFS ® v6.5.4 – the operating system (OS) that provides distributed file system management including a Web Graphical User Interface (GUI) and Command Line Interface (CLI) for TOE management;
- FlexProtect™ – monitors disk and node health, rebuilds failed disks, and preemptively migrates data off of at-risk components;
- SmartConnect™ Advanced – Software module add-on that balances connections to the cluster;
- SyncIQ ® – Software module add-on that provides policy-based file replication, standard disk-to-disk file backup and restores;
- SmartQuotas – Add-on software module that provides quota management and enforces administrator defined storage limits;
- SnapshotIQ™ – Add-on software module that creates a point-in-time copy of any of the shared file directories;
- SmartPools™ – Defines subgroups of nodes, called disk pools, that allow data to be stored and moved according to file attributes; and
- iSCSI – Add-on software module that provides iSCSI targets on the cluster and enables initiators on client computers to send SCSI commands to those targets.

Authenticated administrators can manage the TOE through either the CLI or the Web Administration GUI. Users access the file system through a front end Local Area Network and must authenticate prior to access.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for OneFS is identified in Section 1.5 of the ST.

4 Security Target

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

Title: EMC Corporation Isilon® OneFS® v6.5.4 Security Target
Version: v1.4
Date: 12 April 2012

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.*

OneFS is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2; and
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

OneFS implements a role-based access control policy to control user access to the system, details of this security policy can be found in Section 1.5 of the ST.

In addition, OneFS 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 1.5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of OneFS 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:

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

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is installed on the appropriate, dedicated hardware.
- The TOE is located within a controlled access facility.
- The TOE software will be protected from unauthorized modification.

7.3 Clarification of Scope

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

8 Evaluated Configuration

The evaluated configuration for OneFS comprises:

- The TOE running on one of the Isilon Platform nodes (S Series, X Series, and NL Series)
- Ethernet switches that are non-blocking switch fabric with a minimum 1MB buffer per switch port, and jumbo frame support for front-end network
- One of the following InfiniBand Switches:
    - Cisco SFS 7000 or 7008
    - Flextronics F-X430061, F-X430062, or F-X 430066
    - Mellanox MTS2400
- At least two client systems. One running Microsoft Windows operating system and the other running a Linux operating system.
- An administrator workstation with a web browser such as Internet Explorer, Firefox, Opera, or Safari

The publication entitled OneFS 6.5.4 User Guide describes the procedures necessary to install and operate OneFS in its evaluated configuration.

9 Documentation

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

- OneFS 6.5.4 User Guide 2011
- Isilon Systems S200 Installation and Setup Guide, February 2011
- Isilon IQ Quick Start Guide, Rev A
- Isilon Systems Rail Kit Installation Guide: 1U or 2U Node, Rev A
- Isilon Systems Site Planning and Preparation Guide, September 2011
- OneFS Command Reference Guide v6.5, 2011; and
- EMC Corporation Isilon® OneFS® v6.5.4 Guidance Documentation Supplement v0.2

10 Evaluation Analysis Activities

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

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

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

[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. 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 provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

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

d. Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed;

e. Users and Roles: The objective of this test goal is to ensure the users and roles functionality is correct;

f. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data; and

g. Basic Product Functionality: The objective of this test goal is to exercise the TOE's functionality to ensure that the security claims may not be inadvertently compromised.

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. Accessing the TOE via HTTP instead of HTTPS;

b. Access to the Apache.ini file; and

c. Viewing login page source to glean useful information such as password requirements.

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

11.4 Conduct of Testing

OneFS was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the EMC Quality Assurance facility located in Seattle, Washington. 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 OneFS 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

Supplementary to the audit capabilities, the TOE maintains additional records of events related to the health and performance of a cluster, and these may be viewed through the Web Administration Events tab.

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
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
QA	Quality Assurance
ST	Security Target
TOE	Target of Evaluation

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 Isilon® OneFS® v6.5.4 Security Target, v1.4, 12 April 2012.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of EMC Corporation EMC® Isilon® OneFS® v6.5.4, v0.6, 18 April 2012.