Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Dell EMC™ VxFlex 3.0.1.208 with VxFlex

Ready Node 14G Hardware

9 September 2020

490 EWA 2019

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

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 Centre for Cyber Security (CCCS). 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 Canadian CC Scheme, 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 Canadian Centre for Cyber Security, 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 Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Contact Centre and Information Services
Edward Drake Building
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the 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.

The certification report, certificate of product evaluation and security target are listed on the Certified Products list (CPL) for the Canadian CC Scheme and posted on the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Dell EMC™ VxFlex 3.0.1.208 with VxFlex Ready Node 14G Hardware (hereafter referred to as the Target of Evaluation, or TOE), from Dell EMC , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 9 September 2020 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for TOE, 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.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian CC Scheme and the Common Criteria portal (the official website of the International Common Criteria Project).

1   IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1:   TOE Identification

TOE Name and Version	Dell EMC™ VxFlex 3.0.1.208 with VxFlex Ready Node 14G Hardware
Developer	Dell EMC

1.1   COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

EAL 2+ (ALC_FLR.2)

1.2   TOE DESCRIPTION

The TOE is a combined software and hardware TOE. The VxFlex operating system (OS) is the VxFlex software component which provides the ability to use existing servers' local disks and local area network resources to create a virtual Storage Area Network. The VxFlex OS utilizes the existing local storage devices and turns them into shared block storage. The VxFlex Ready Node is the combination of VxFlex OS software-defined block storage and Dell PowerEdge servers, optimized to run VxFlex OS. The TOE is managed by the VxFlex OS Graphical User Interface (GUI) and VxFlex OS Command Line Interface (CLI). Communications between the TOE and remote administrators are protected using TLS.

1.3   TOE ARCHITECTURE
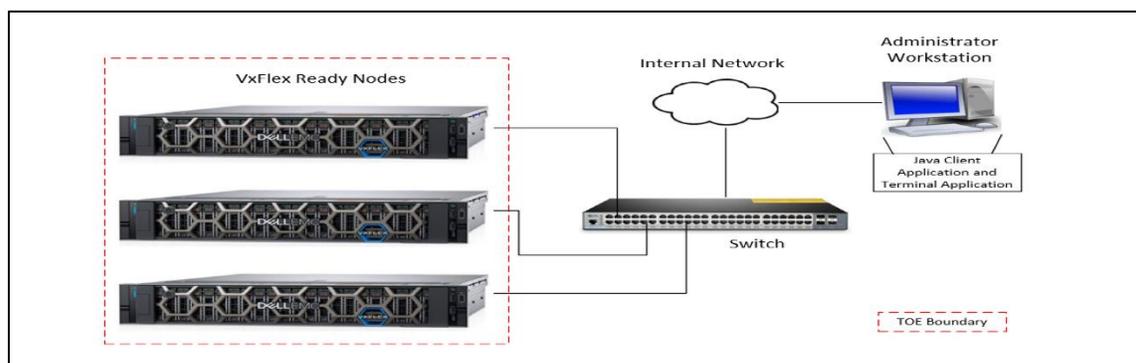
A diagram of the TOE architecture is as follows:

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementation have been evaluated by the CMVP and is used by the TOE:

Table 2: Cryptographic Implementation

Cryptographic Module/Algorithm	Certificate Number
OpenSSL FIPS Object Module version 2.0.8 Cryptographic Module	1747

3   ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE 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.

3.1   USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

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

- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

- The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.

3.2   CLARIFICATION OF SCOPE

The following features are excluded from this evaluation:

- The TOE supports REST clients; however, no REST clients are implemented in the evaluated configuration.

- The TOE supports a vCenter Plugin GUI required for installation and setup. Once setup is complete, this interface is not used in the evaluated configuration. Access to this interface requires vCenter admin credentials.

- The following deployment options are supported but not implemented in the evaluated configuration:

  - Storage Data Server (SDS), Storage Data Client (SDC), and Meta Data Manager (MDM) instances on physical servers running CentOS, Red Hat, SUSE, and Windows.

  - SDS, SDC, and MDM instances on Hyper-V, XenServer, and Redhat KVM hypervisors.

  - Automated Management Service.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises the VxFlex operating system version 3.0.1 build 208 running on the following Ready Node Servers:

- R640
- R740xd
- R840

The Ready Node Servers run ESXi 6.7.0-20190802001and vCenter Server Appliance v6.7u3b.

A management workstation running Windows 10, Java Client application and JRE 8.0.2210.11 is required in the operational environment.

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) Dell EMC VxFlex OS, Version 3.x, CLI Reference Guide, March 2019
b) Dell EMC VxFlex OS, Version 3.x, Monitor, March 2019
c) Dell EMC VxFlex OS, Version 3.x, Deploy Dell EMC VxFlex OS, April 2019
d) Dell EMC VxFlex OS, Version 3.x, Security Configuration Guide, March 2019
e) Dell EMC VxFlex Ready Node 14th generation servers, Server Installation Guide, April 2019
f) Dell EMC VxFlex Ready Node R640/R740xd, Operating System Installation and Configuration Guide – ESXI Servers, June 2019
g) Dell EMC VxFlex Ready Node R840, Operating System Installation and Configuration Guide, April 2019
h) Dell EMC™ VxFlex 3.0.1 Common Criteria Guidance Supplement, Version 1.0, 31 July 2020.

5   EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1   DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2   GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

5.3   LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE 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 the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

6.1 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 Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE 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.

6.3 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. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests;

b. Verification of Cryptographic Implementation: The evaluator verified the presence of claimed cryptographic module used by the TOE;

c. Audit: The evaluator confirmed that appropriate audit records are generated for start up and shutdown of the audit function;

d. Session Timeout: The evaluator confirmed that time interval for the command line interface idle timeout can be configured;

e. Account Management: The evaluator confirmed that a new user cannot be created without a role assignment; and

f. Password Policy: The evaluator confirmed that a password policy can be enforced by the TOE.

6.3.1 FUNCTIONAL TEST RESULTS

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

6.4   INDEPENDENT PENETRATION TESTING

The penetration testing effort focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2).   Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4).   Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their penetration testing effort.

6.4.1   PENETRATION TEST RESULTS

Type 1 & 2 searches were conducted on 7/27/2020 and included the following search terms:

- VxFlex and/or VxFlex Vulnerability

Vulnerability searches were conducted using the following sources:

- National Vulnerability Database
- EMC Support
- Common Vulnerabilities and Exposures

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

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 Centre for Cyber Security (CCCS). This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

- It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CCCS	Canadian Centre for Cyber Security
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
MDM	Meta Data Manager
PP	Protection Profile
SDC	Storage Data Client
SDS	Storage Data Server
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Dell EMC™ VxFlex 3.0.1 Security Target, Version 1.1, August 8, 2020.
Evaluation Technical Report for Common Criteria Evaluation of Dell EMC VXFlex 3.0.1, Version 1.2, September 9, 2020.