Certification Report

EMC® NetWorker® v8.0.1.4

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-242-CR
Version: 1.0
Date: 27 November 2013
Pagination: i to iii, 1 to 10

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, 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.

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 27 November 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:

- NetWorker is a registered trademark of EMC Corporation; and
- EMC is a registered trademark of EMC Corporation.

TABLE OF CONTENTS

Executive Summary

EMC® NetWorker® v8.0.1.4 (hereafter referred to as EMC NetWorker), from EMC Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

EMC NetWorker is a network-based backup software solution that centralizes, automates, and accelerates data backup and recovery across the IT environment. EMC NetWorker provides data protection for a variety of operating systems and data types. EMC NetWorker reproduces online file system data at a protected location, while it maintains location and obsolescence tracking information about the data. EMC NetWorker can then re-create the data if the online version is inadvertently changed, lost, or corrupted.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 29 October 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 EMC NetWorker, 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*The following augmentation is claimed: ALC_FLR..2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the EMC NetWorker 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® NetWorker® v8.0.1.4 (hereafter referred to as EMC NetWorker), from EMC Corporation.

2 TOE Description

EMC NetWorker is a network-based backup software solution that centralizes, automates, and accelerates data backup and recovery across the IT environment. EMC NetWorker provides data protection for a variety of operating systems and data types. EMC NetWorker reproduces online file system data at a protected location, while it maintains location and obsolescence tracking information about the data. EMC NetWorker can then re-create the data if the online version is inadvertently changed, lost, or corrupted.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for EMC NetWorker is identified in Section 6 of the (ST).

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in EMC NetWorker:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	NIST SP 800-67	690, 707, 1147, 1268
Advanced Encryption Standard (AES)	FIPS 197	810, 860, 1171, 1951
(RSA) Rivest Shamir Adleman	FIPS 186-2	338, 339
DSA (Digital Signature Algorithm)	FIPS 186-3	300, 311, 554, 623, 92, 93, 98, 100, 239, 240, 281, 282
RSA (Rivest, Shamir, Adleman)	RSASSA-PKS#1 v1.5 RSASSA-PSS	390, 412, 887, 1012
PRNG (Pseudorandom Number Generator)	FIPS 186-2	466, 492, 943, 1027
DRBG (Deterministic Random Bit Generator)	NIST SP 900-90A	2, 4, 122, 172
Secure Hash Algorithm (SHA-1)	FIPS 180-4	807, 855, 1555, 1713
Hash Message Authentication Code (HMAC)	FIPS 198-1	449, 477, 1040, 1177

4 Security Target

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

Title: EMC® NetWorker® v8.0.1.4 Security Target
Version: 1.1
Date: 29 October 2013

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 NetWorker is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST:
    • EXT_FRU_DRP – Data Retention Periods.
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

EMC NetWorker implements an access control policy to control access to the system; details of this security policy can be found in Section 6 of the ST.

In addition, EMC NetWorker implements other policies pertaining to security audit, cryptographic support, user data protection, identification and authentication, security management, protection of the TSF, resource utilization and TOE access. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of EMC NetWorker 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 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, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation; and
- The TOE will be protected from unauthorized modification.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The IT environment will provide the TOE with the necessary reliable timestamp.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access; and
- The TOE is installed on the appropriate, dedicated hardware and operating system.

7.3 Clarification of Scope

EMC NetWorker incorporates CAVP-validated cryptography and was not subjected to CMVP FIPS-140 validation.

8 Evaluated Configuration

The evaluated configuration for EMC NetWorker comprises:

The TOE is a distributed software-based application, EMC NetWorker v8.0.1.4, comprised of the following:

- NetWorker Management Console (NMC) Applet v8.0.1.4 build 163 on General Purpose Computer (GPC) hardware running Windows 7 SP1.
- NetWorker Management Console (NMC) Server v8.0.1.4 build 163 on GPC Hardware running Windows Server 2008 R2 SP1.
- NetWorker Server v8.0.1.4 build 163 on GPC Hardware running Windows Server 2008 R2 SP1.
- NetWorker Client v8.0.1.4 build 163 on GPC hardware running either Microsoft Windows 2008 R2 SP1 or Red Hat Enterprise Linux 6.
- NetWorker Storage Node v8.0.1.4 build 163 on GPC Hardware running Windows Server 2008 R2 SP1.

The publications entitled EMC® NetWorker® Release 8.0 Service Pack 1 Installation Guide and EMC Corporation EMC NetWorker v8.0.1.4 Guidance Documentation Supplement v0.4 describe the procedures necessary to install and operate EMC NetWorker in its evaluated configuration.

9 Documentation

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

a. EMC® NetWorker® Release 8.0 Service Pack 1 Administration Guide, P/N 300-999-719, REV A01;
b. EMC® NetWorker® Release 8.0 Service Pack 1 Command Reference Guide, P/N 300-999-721, REV A01;
c. EMC® NetWorker® Release 8.0 Service Pack 1 Error Message Guide, P/N 300-999-724, REV A01;
d. EMC® NetWorker® Release 8.0 Service Pack 1 Installation Guide, P/N 300-999-725, REV A01;
e. EMC® NetWorker® 8.0.1.4 Guidance Documentation Supplement v0.4
f. EMC® NetWorker® Release 8.0 and Service Packs Release Notes, P/N 300-013-567, REV A05, December 14, 2012; and
g. EMC® NetWorker® 8.0 Cumulative Hotfixes, April 2013.

10 Evaluation Analysis Activities

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

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

The evaluators reviewed the flaw remediation procedures used by developer for the EMC NetWorker. 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 NetWorker. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify EMC NetWorker potential vulnerabilities. The evaluators identified potential vulnerabilities; subsequent to follow-on penetration testing (ref: section 11.3) it was verified that none of the potential vulnerabilities were exploitable in the operational environment for EMC NetWorker.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing 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.

[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.

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

c. Access of Private Key from Storage Node: The objective of this test goal is to verify that the private key used for daemon authentication is not visible through the Storage Node Command Line Interface (CLI);

d. Management of Security Attributes: and

    a. Security Administrator: The objective of this test goal is to verify that the security administrator is able to perform the operations as specified in the ST;

    b. Application Administrator: The objective of this test goal is to verify that the application administrator is able to perform the operations as specified in the ST;

    c. Audit Log Management: The objective of this test goal is to verify that the security administrator is able to perform the audit log operations as specified in the ST;

e. Roles and Permissions: The objective of this test goal is to verify that select users are able to perform operations as specified in the roles and permissions attributed in the ST.

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. Tool Scanning: The objective of this test goal is to use Nessus to scan for potential vulnerabilities;

b. Information Leak verification: The objective of this test goal is to verify, using wireshark, that traffic between the NetWorker Server and NetWorker Storage Node is protected;

c. Concurrent User Login: The objective of this test goal is to verify that concurrent administrator login does not compromise the NetWorker system;

d. Power Failure: The objective of this test goal is to verify that a power failure does not compromise the NetWorker system;

e. Backup with insufficient space: The objective of this test goal is to verify that an attempt to backup data to a device with insufficient space does not compromise the NetWorker system;

f. Restore file Permissions: The objective of this test goal is to verify that a client can only restore files for which that user has permissions;

g. Invalid Data in CLI: The objective of this test goal is to verify that entering invalid data will not create an invalid user; and

h. Bypassability: The objective of this test goal is to attempt to bypass the TOE Security Functions.

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

11.4 Conduct of Testing

EMC NetWorker was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the developer's site. located at at 1111 International Blvd, Burlington, Ontario. 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 EMC NetWorker 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

Note the inclusion of the encryption directive file during initial configuration of the NetWorker client. Instructions for creating this directive may be found in the Guidance Supplement, and must be followed to ensure protection of data between the parts of the TOE. Customers without previous NetWorker experience may find it useful to engage EMC Professional Services to ensure adherence to the evaluated configuration.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
3DES	Triple-Data Encryption Standard
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
HMAC	Hash Message Authentication Code
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NMC	Networker Management Console
PALCAN	Program for the Accreditation of Laboratories - Canada
PRNG	Pseudorandom Number Generator
RSA	Rivest, Shamir, Aldeman
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm
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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. EMC® NetWorker® v8.0.1.4 Security Target, 1.1, 29 October 2013.

e. Evaluation Technical Report EMC® NetWorker® v8.0.1.4, 29 October 2013, v3.1.