Certification Report

EAL 2+ Evaluation of EMC® Avamar® v6.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-212-CR
Version: 1.0
Date: 12 October 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, Ontario.

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 12 October 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 registered trademarks:

- EMC and Avamar are trademarks or registered trademarks of EMC Corporation in the United States and other countries.

TABLE OF CONTENTS

Executive Summary

EMC® Avamar® v6.1 (hereafter referred to as Avamar® v6.1), from EMC, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Avamar® v6.1 is a backup and recovery software TOE that uses data deduplication technology to reduce daily backups before transferring across the network for storage on disk. Deduplication breaks data into variable length segments and eliminates redundant sub-file data segments. Each data segment is assigned a unique ID which the TOE uses to compare it to other data segments that are already backed up. Only new data is transferred for back up.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 31 August 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 Avamar® v6.1, 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: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Avamar® v6.1 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® Avamar® v6.1 (hereafter referred to as Avamar® v6.1), from EMC.

2 TOE Description

Avamar® v6.1 is a deduplication backup and restore software TOE that runs on EMC Avamar Data Store Gen 4 hardware appliances (nodes). Deduplication breaks data into variable length segments and eliminates redundant sub-file data segments. Each data segment is assigned a unique ID which the TOE uses to compare it to other data segments that are already backed up. Only new data is transferred for back up. The TOE is deployed on a network in a client-server configuration and can be deployed in a single-node configuration, with the utility and storage nodes combined on one server or in a multi-node configuration with one utility node, three storage nodes, and a remote single-node server.The evaluated TOE was installed EMC Avamar® Data Store Gen 4 hardware appliances in both a multi-node and single-node configuration.

A detailed description of the Avamar® v6.1 architecture is found in Section 1.4 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Avamar® v6.1 is identified in Section 6 of the ST.

4 Security Target

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

Title: EMC Corporation EMC® Avamar® v6.1 Security Target
Version: 1.0
Date: 20 August 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.*

Avamar® v6.1 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_FDD_DDR.1 - Duplicate data removal.
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

Avamar® v6.1 implements a Server Access Control policy to control how administrators and operators access the TOE and a Client Access Control policy to control how users access the TOE through a client system; details of these security policies can be found in Section 6 of the ST.

In addition, Avamar® v6.1 implements policies pertaining to security audit, user data protection, identification and authentication, security management, protection of the TOE Security Functionality (TSF) and user data deduplication. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Avamar® v6.1 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:

- Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The physical environment must be suitable for supporting a computing device in a secure setting;

- The TOE environment must provide reliable timestamps to the TOE;

- The TOE environment must protect itself and the TOE from external interference or tampering;
- The TOE hardware and client OS must support all required TOE functions;
- The TOE environment must provide identification and authentication mechanisms if required for user access to TOE; and
- The TOE environment must provide a secure connection for client systems and remote administrators to access the TOE.

7.3 Clarification of Scope

Avamar® v6.1 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. Avamar® v6.1 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 Avamar® v6.1 comprises:

- Avamar Multi-Node Server build 6.1.0-402;
- Avamar Single-Node Server build 6.1.0-402;
- NDMP Accelerator 6.1.0-402 build;
- VMware Backup Agent Application build 6.1.0-402;
- avtar 32 bit Windows client build 6.1.100-402;
- avtar 64 bit Windows client build 6.1.100-402;
- avtar 32 bit Linux client build 6.1.100-402;
- avtar 64 bit Linux client build 6.1.100-402; and
- avtar Desktop/Laptop client build 6.1.0.4.24.3.

The TOE server components run on EMC Avamar Data Store Gen4 servers. The VMware Backup Agent Application runs on ESXi5.0.0. The TOE client components run on Microsoft Windows XP 32-bit, Microsoft Windows 7 64-bit, Red Hat Enterprise Linux 4.0 Update 8 32-bit, SuSE Linux 11.0 Service Pack 1 64-bit.

The publication entitled EMC Corporation Avamar v6.1 Guidance Documentation Supplement, v0.1 describes the procedures necessary to install and operate Avamar® v6.1 in its evaluated configuration.

9 Documentation

The EMC documents provided to the consumer are as follows:

a. EMC Avamar v6.1 Administration Guide, REV A01;

b. EMC Avamar 6.1 Backup Clients Guide, REV A01;

c. Avamar v6.1 and Data Domain Integration Guide, REV A01;

d. EMC Avamar 6.1 for Lotus Domino Guide, REV A01;

e. EMC Avamar v6.1 for IBM DB2 Guide, REV A01;

f. EMC Avamar v6.1 for Exchange VSS Guide, REV A01;

g. EMC Avamar v6.1 for Hyper-V VSS Guide, REV A01;

h. EMC Avamar 6.1 Data Store Gen4 Multi-Node System Installation, REV A04;

i. EMC Avamar 6.1 Data Store Gen4 Single-Node Customer Installation Guide, REV A03;

j. EMC Avamar v6.1 Management Console Command Line Interface (MCCLI) Programmer Guide, REV A01;

k. EMC Avamar v6.1 NDMP Accelerator Guide, REV A01;

l. EMC Avamar v6.1 Operational Best Practices, REV A01;

m. EMC Avamar v6.1 for Oracle Guide, REV A01;

n. EMC Avamar v6.1 Product Security Guide, REV A01;

o. EMC Avamar v6.1 Release Notes, REV A01, April 19, 2012;

p. EMC Avamar v6.1 for SAP with Oracle Guide, REV A01;

q. EMC Avamar Data Store Site Prep Technical Specifications, REV A09;

r. Avamar v6.1 for SharePoint VSS Guide, REV A01;

s. EMC Avamar v6.1 for SQL3 Server Guide, REV A01;

t. EMC Corporation Avamar v6.1 Guidance Documentation Supplement, v0.1, May 22, 2012;

u. SVR-D2U-R510 Installation and Replacement Guide, Rev A02;

v. EMC Avamar v6.1 for Sybase ASE User Guide, REV A01;

w. EMC Avamar v6.1 for VMware Guide, REV A01; and

x. EMC Avamar v6.1 for Windows Servers Guide, REV A01.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Avamar® v6.1, including the following areas:

Development: The evaluators analyzed the Avamar® v6.1 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 Avamar® v6.1 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 Avamar® v6.1 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 Avamar® v6.1 configuration management system and associated documentation was performed. The evaluators found that the Avamar® v6.1 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 Avamar® v6.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by EMC for Avamar® v6.1. 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 Avamar® v6.1. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Avamar® v6.1 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to Avamar® v6.1 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:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Audit: The objective of this test goal is to verify the presence and content of the audit logs;

[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.

c. Unauthenticated Backup and Restore: The objective of this test goal is to verify that the ability to backup user data without authentication is limited to a client;

d. Protection of the TSF: The objective of this test goal is to verify that the nodes within a server are connected via dedicated Ethernet; and

e. Deduplication: The objective of this test goal is to verify that the deduplication functionality does not introduce errors and that the integrity of deduplicated data is preserved.

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 test focused on:

a. Direct Attack on Backup Functionality: The objective is to verify that a backup operation, if intercepted, cannot be used to access user information.

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

11.4 Conduct of Testing

Avamar® v6.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the developer's testing facility located in Irvine, California. 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 Avamar® v6.1 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

The documentation set for EMC Avamar provides a mature, comprehensive set of instructions for planning, installation and operation. It is strongly recommended that users of the TOE take care to consult the documentation that applies to their particular implementation.

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
OS	Operating System
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 EMC® Avamar® v6.1 Security Target, Version 1.0, 20 August 2012.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of EMC® Avamar® v6.1, Version 0.3, 31 August 2012.