Certification Report

EAL 2+ Evaluation of EMC® Atmos™ v2.0.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-151-CR
Version: 1.0
Date: 2 March 2012
Pagination: i to iii, 1 to 8

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 2 March 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:

- Atmos is a trademark of EMC Corporation;
- Linux is a registered trademark of Linus Torvalds Inc.;
- VMware is a registered trademark of VMware, Inc.;
- EMC Corporation is a registered trademark of EMC Corporation; and
- EMC is a registered trademark of EMC Corporation.

TABLE OF CONTENTS

Executive Summary

EMC® Atmos™ v2.0.1 (hereafter referred to as Atmos™ v2.0.1), from EMC Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Atmos™ v2.0.1 is a software-only TOE that is implemented in the EMC Corporation product lines: EMC Atmos, which is a series of stand-alone servers; and EMC Atmos Virtual Edition (VE) that runs on VMware ESX. EMC Atmos is a server system for information storage that is used as an infrastructure for building cloud storage solutions.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 15 February 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 Atmos™ v2.0.1, 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 Atmos™ v2.0.1 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® Atmos™ v2.0.1 (hereafter referred to as Atmos™ v2.0.1), from EMC Corporation.

2 TOE Description

Atmos™ v2.0.1 is a software-only TOE that is implemented in the EMC Corporation product lines: EMC Atmos, which is a series of stand-alone servers; and EMC Atmos Virtual Edition (VE), that runs on VMware ESX 4.0. EMC Atmos is a server system for information storage that is used as an infrastructure for building cloud storage solutions.

The TOE comprises the major components Atmos Software v2.0.1 and rPath Linux v2 OS.

Atmos Software v2.0.1 provides the server functionality for the TOE that includes data replication, de-duplication, compression, retention and deletion functionality. The administrator interface is web-based, allowing the administrator to configure the TOE, provision users, and assign roles.

rPath Linux v2 OS provides the operating system functionality for the TOE including identification and authentication of local login accounts for installation, configuration, and maintenance tasks carried out using the TOE command line interface (CLI).

A comprehensive TOE description may be found in Section 1.5 of the ST.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Atmos™ v2.0.1 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® Atmos™ v2.0.1 Security Target
Version: 0.14
Date: 2 February 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.*

Atmos™ v2.0.1 is:

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

Atmos™ v2.0.1 controls access to user data and metadata by enforcing the Atmos Discretionary Access Control policy. Access to user data and metadata is controlled by the user's assigned role, UID [2], and object ACL [3].

In addition, Atmos™ v2.0.1 implements policies pertaining to security audit, user data protection, identification and authentication, security management, protection of the TSF [4], and resource utilization.

Further details on these security policies may be found in Section 1.5.2 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Atmos™ v2.0.1 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:

- There are competent individuals assigned to manage the TOE and the security of the information it contains. These individuals are non-hostile, trained, and follow all supplied guidance.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

[2] User Identification

[3] Access Control List

[4] TOE Security Functionality

- The components of the TOE critical to security policy enforcement are located within controlled access facilities that will be protected from unauthorized physical access and modification; and

- The IT environment provides the TOE with the necessary reliable timestamps.

7.3 Clarification of Scope

Atmos™ v2.0.1 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. Atmos™ v2.0.1 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 Atmos™ v2.0.1 comprises:

- Atmos Software v2.0.1 and rPath Linux v2 OS running on Atmos appliance models: WS-120, WS-240, and WS-360; and

- Atmos Software v2.0.1 and rPath Linux v2 OS running on VMware ESX Server 4.0.

The publication entitled *EMC Corporation Atmos v2.0.1 Guidance Documentation Supplement* describes the procedures necessary to install and operate Atmos™ v2.0.1 in its evaluated configuration.

9 Documentation

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

- EMC® Atmos™ v2.0 Administrator's Guide;

- EMC® Atmos™ v2.0 Programmer's Guide;

- EMC® Atmos™ v2.0 Security Configuration Guide;

- EMC® Atmos™ v2.0 Non-EMC Software License Agreements;

- EMC® Atmos™ v2.0.1 Physical Hardware Installation Procedures;

- EMC® Atmos™ v2.0.1 Virtual Edition Installation Procedures;

- EMC® Atmos™ v2.0.1 Release Notes; and

- EMC Corporation Atmos v2.0.1 Guidance Documentation Supplement.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Atmos™ v2.0.1, including the following areas:

Development: The evaluators analyzed the Atmos™ v2.0.1 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 Atmos™ v2.0.1 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 Atmos™ v2.0.1 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 Atmos™ v2.0.1 configuration management system and associated documentation was performed. The evaluators found that the Atmos™ v2.0.1 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 Atmos™ v2.0.1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for Atmos™ v2.0.1. 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 Atmos™ v2.0.1. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Atmos™ v2.0.1 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to Atmos™ v2.0.1 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[5].

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:

- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;
- Password change utility: The objective of this test goal is to verify that an administrator password is changed on all nodes in a multi-node[6]configuration;
- System hardening: The objective of this test goal is to verify that the rPath Linux v2 OS hardening feature is functioning correctly;
- Session timeout: The objective of this test goal is to verify the administrator login session will time out after the predetermined period of inactivity; and

[5] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

[6] Atmos™ v2.0.1 can be configured in a distributed multi-server or multi-node configuration, with a single primary node.

- Audit collection: The objective of this test case is to verify that audit files are collected from all distributed nodes by the primary node.

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 with penetration testing focused on password enforcement.

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

11.4 Conduct of Testing

Atmos™ v2.0.1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the developers Quality Assurance (QA) facility in Cambridge, Massachusetts. 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 Atmos™ v2.0.1 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

Atmos™ v2.0.1 relies upon an external Simple Mail Transfer Protocol (SMTP) server to deliver alert messages and forgotten passwords for administrators, and an external Network Time Protocol (NTP) server to provide the TOE with reliable time stamps.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CIFS	Common Internet File System

Acronym/Abbreviation/ Initialization	Description
CLI	Command Line Interface
CPL	Certified Products list
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
NTP	Network Time Protocol
PALCAN	Program for the Accreditation of Laboratories - Canada
QA	Quality Assurance
SMTP	Simple Mail Transfer Protocol
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VE	Virtual Edition

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® Atmos™ v2.0.1 Security Target, 0.14, 2 February 2012.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of EMC Corporation® Atmos™ v2.0.1, Version 1.4, 15 February 2012.