Certification Report

EAL 2+ Evaluation of FortiAnalyzer™ v4.0 MR3

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-324-CR
Version: 1.0
Date: 11 June 2014
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 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, 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, 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.

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 11 June 2014, 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 trademark:

- FortiAnalyzer™ is a registered trademark of Fortinet, Incorporated.

TABLE OF CONTENTS

Executive Summary

FortiAnalyzer™ v4.0 MR3, from Fortinet, Incorporated, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

FortiAnalyzer™ v4.0 MR3 is a log collection and reporting device. FortiAnalyzer units are network appliances that provide integrated log collection and reporting tools. Logs for email, File Transfer Protocol (FTP), web browsing, security events, and other network activity are analyzed to aid in the identification of security issues.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 3 June 2014 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 FortiAnalyzer™ v4.0 MR3, 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.1 – Basic Flaw Remediation.

Communications Security Establishment, as the CCS Certification Body, declares that the FortiAnalyzer™ v4.0 MR3 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 FortiAnalyzer™ v4.0 MR3, from Fortinet, Incorporated.

2 TOE Description

FortiAnalyzer™ v4.0 MR3 is a log collection and reporting device. FortiAnalyzer units are network appliances that provide integrated log collection and reporting tools. Logs for email, File Transfer Protocol (FTP), web browsing, security events, and other network activity are analyzed to aid in the identification of security issues. The appliances support secure communication between the TOE and the monitored devices, and between the TOE and its remote administrators using FIPS 140-2 validated cryptography.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for FortiAnalyzer™ v4.0 MR3 is identified in Section 6 of the ST.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
FortiAnalyzer 4.0 MR3	2105
FortiAnalyzer-4000B	2115

4 Security Target

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

Title: Security Target for FortiAnalyzer™ v4.0 MR3 Centralized Reporting
Version: 1.0
Date: 3 June 2014

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.*

FortiAnalyzer™ v4.0 MR3 is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - EXT_DCR_AGG.1 – Aggregation;
   - EXT_DCR_COL.1 – Data Collection;
   - EXT_DCR_QUA.1 – Quarantine; and
   - EXT_DCR_REP.1 – Reporting.

b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

c. *Common Criteria EAL augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

FortiAnalyzer™ v4.0 MR3 implements access control policies for administrators for devices. Administrative users are granted access to data based on the permissions in their access profile. Devices that are monitored by the TOE must first be registered with the TOE in order to communicate with the TOE. Details of these security policies can be found in Section 6 of the ST.

In addition, FortiAnalyzer™ v4.0 MR3 implements policies pertaining to security audit, cryptographic support, identification and authentication, security management, protection of the TOE Security Functions (TSF), trusted path, and data collection and reporting. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of FortiAnalyzer™ v4.0 MR3 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 are one or more competent individuals assigned to manage the TOE.

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

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

- The TOE is connected to the network in such a way that it is able to access all of the monitored resources.

8 Evaluated Configuration

The evaluated configuration for FortiAnalyzer™ v4.0 MR3 comprises:

Product	Firmware Version	Hardware Version
FortiAnalyzer™	Version 4.0 MR3 build 3059, 130918	100C
		200D
		400B
		400C
		1000C
		2000B
		4000B

9 Documentation

The Fortinet, Incorporated documents provided to the consumer are as follows:

a. FortiAnalyzer Administration Guide Version 4.0 MR3;

b. FortiAnalyzer CLI Reference Version 4.0 MR3;

c. FortiAnalyzer Log Message Reference Version 4.0 MR3; and

d. FortiAnalyzer Install Guide Version 4.0 MR3.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of FortiAnalyzer™ v4.0 MR3, including the following areas:

Development: The evaluators analyzed the FortiAnalyzer™ v4.0 MR3 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 FortiAnalyzer™ v4.0 MR3 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 FortiAnalyzer™ v4.0 MR3 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 FortiAnalyzer™ v4.0 MR3 configuration management system and associated documentation was performed. The evaluators found that the FortiAnalyzer™ v4.0 MR3 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 FortiAnalyzer™ v4.0 MR3 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Fortinet, Incorporated for FortiAnalyzer™ v4.0 MR3. 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 FortiAnalyzer™ v4.0 MR3. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify FortiAnalyzer™ v4.0 MR3 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to FortiAnalyzer™ v4.0 MR3 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. Identification and Authentication: The objective of this test case is to validate that the user is authenticated prior to gaining access a TOE service and that no TOE service or data is available prior to user authentication;

c. Alerts: The objective of this test case is to verify that alerts can be sent to an email address;

d. Log Data: The objective of this test case is to verify that authorized administrators can access log data and delete log data;

e. Trusted Path: The objective of this test case is to verify that the TOE uses SSL/TLS 1.0 for the web-based GUI, and SSH with approved algorithms for CLI access to communicate with remote consoles;

f. Security Roles: The objective of this test case is to verify that administrator accounts and access profiles can be created, modified, and deleted;

[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.

g. Data Aggregation: The objective of this test case is to verify that the TOE can aggregate data from monitored devices for analysis and reporting;

h. Data Collection: The objective of this test case is to verify that the TOE can collect specified data from remote devices; and

i. Reporting: The objective of this test case is to verify that the TOE can create and run reports based on specific parameters.

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. Port Scanning: The objective of this test was to scan the TOE using a port scanner to determine what ports were open and what services were running;

b. Buffer Overflow: The objective of this test is to determine if TOE is susceptible to a known vulnerability (CVE-2007-2446) which would allow remote attackers to execute arbitrary code;

c. SSH version corruption: The objective of this test is to determine if TOE will respond to SSH requests with corrupted version stings;

d. Key Access: The objective of this test is to attempt to scan, locate and utilize private and public keys stored on the TOE;

e. Login attacks: The objective of this test is to determine whether the TOE is susceptible to attacks on SSH, HTTP, and HTTPS logins;

f. Memory Corruption: The objective of this test is to determine whether the TOE is susceptible to a known memory corruption vulnerability which could allow the execution of arbitrary code;

g. Denial of Service: The objective of this test is to determine whether the TOE is susceptible to denial of service attacks;

h. Directory Traversal: The objective of this test is to determine whether the TOE is susceptible to directory traversal attacks which could allow unauthorized access to restricted directories and files; and

i. SQL Injection: The objective of this test is to determine whether the TOE is susceptible to SQL injection attacks.

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

11.4 Conduct of Testing

FortiAnalyzer™ v4.0 MR3 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at EWA-Canada. The CCS Certification Body witnessed a portion of the independent testing. 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 FortiAnalyzer™ v4.0 MR3 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 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products List
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing

Acronym/Abbreviation/ Initialization	Description
PALCAN	Program for the Accreditation of Laboratories - Canada
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation

14 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. Security Target for FortiAnalyzer™ v4.0 MR3 Centralized Reporting, version 1.0, 3 June 2014.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of Fortinet, Incorporated FortiAnalyzer™ v4.0 MR3 Centralized Reporting Document No. 1734-000-D002, Version 1.0, 3 June 2014.