Reference: 2017-48-INF-3131-v1
Target: Pœblico
Date: 12.05.2020

Created by: CERT9
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2017-48**
TOE	**Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)**
Applicant	**770560389Z - Fortinet, Inc.**
References	

[EXT-3621] Solicitud Certificacion FORTINET Fortimanager 5.6.1

Certification report of the product “Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)”, as requested in [EXT-3621] dated 11/10/2017, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-5863] received on 03/04/2020.

CONTENTS

EXECUTIVE SUMMARY 3
TOE SUMMARY 3
SECURITY ASSURANCE REQUIREMENTS 4
SECURITY FUNCTIONAL REQUIREMENTS 5
IDENTIFICATION 5
SECURITY POLICIES 5
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT 6
CLARIFICATIONS ON NON-COVERED THREATS 6
OPERATIONAL ENVIRONMENT FUNCTIONALITY 6
ARCHITECTURE 6
LOGICAL ARCHITECTURE 6
PHYSICAL ARCHITECTURE 7
DOCUMENTS 7
PRODUCT TESTING 8
EVALUATED CONFIGURATION 8
EVALUATION RESULTS 9
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM 9
CERTIFIER RECOMMENDATIONS 9
GLOSSARY 10
BIBLIOGRAPHY 10
SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE) 10
RECOGNITION AGREEMENTS 11
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) 11
International Recognition of CC – Certificates (CCRA) 11

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product “Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)”.

The TOE is the firmware deployed in a family of Fortinet appliances which is intended to provide network management capabilities over one or more Fortinet network security devices.

Developer/manufacturer: Fortinet, Inc.

Sponsor: Fortinet, Inc..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL4 + ALC_FLR.3.

Evaluation end date: 04/02/2020.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.3) have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 + ALC_FLR.3, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product “Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)”, a positive resolution is proposed.

TOE SUMMARY

The TOE is the firmware “Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)”. This firmware provides network management capabilities over one or more Fortinet network security devices when it is installed in the corresponding Fortinet hardware platform and it is running in stand-alone ‘FIPS-CC’ mode.

Authorized administrators are able to configure and manage devices, using functions that include verification and update of firmware and license information. Administrators can create and modify policies and objects and push them to the devices. The TOE is able to retrieve up-to-date antivirus and intrusion prevention signatures from Fortinet’s FortiGuard service to push to the managed devices.

The TOE is capable of grouping devices into administrative domains (ADOMs), which simplifies the application of policies, distribution of content security and firmware updates for large implementations. ADOMs are implemented in the evaluated configuration.

The TOE has extensive logging capabilities which include the logging of administrative actions and logging of use of the trusted cryptographic channels.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional component ALC_FLR.3, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE.TSS.1
ADV	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_FLR.3
	ALC_LCD.1
	ALC_TAT.1
ATE	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.3

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5.

SECURITY FUNCTIONAL REQUIREMENTS
FAU_GEN.1
FAU_GEN.2
FAU_SAR.1
FAU_SAR.2
FCS_CKM.1(1)
FCS_CKM.1(2)
FCS_CKM.1(3)
FCS_CKM.4
FCS_COP.1
FDP_ACC.1
FDP_ACF.1
FIA_AFL.1
FIA_SOS.1
FIA_UAU.2
FIA_UID.2
FMT_MSA.1
FMT_MSA.3
FMT_MTD.1
FMT_SMF.1
FMT_SMR.1
FPT_ITC.1
FPT_STM.1
FTA_SSL.3
FTP_ITC.1
FTP_TRP.1

IDENTIFICATION

Product: “Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)”

Security Target: Fortinet FortiManager 5.6.6 Security Target v1.13 (21 October 2019).

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL4 + ALC_FLR.3.

SECURITY POLICIES

The use of the product “Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)” shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in [ST], chapter 3.2 (Organizational security policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.3 (Assumptions) are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.1 (Threats) do not suppose a risk for the product "Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)", although the agents implementing attacks have the attack potential according to the Enhanced-Basic of EAL4 + ALC_FLR.3 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are detailed in [ST], chapter 4.2 (Security objectives for the operational environment).

ARCHITECTURE

LOGICAL ARCHITECTURE

The main TOE capabilities are:

- **Security Audit**. The TOE generates audit records for security relevant events. An Administrator2 may view the contents of the audit records; however, this functionality is restricted to those users authorized to view the records.
- **Cryptographic Support**. The TOE provides key generation, key destruction and cryptographic operation functions supported by Cryptographic Algorithm Validation Program (CAVP)- validated algorithms.

- **User Data Protection**. The TOE controls access to the security data required to perform security management functions including management of devices.
- **Identification and Authentication**. All TOE administrative users must be identified and authenticated. Users are locked out after a number of unsuccessful authentication attempts. Administrator passwords must meet the configured length and composition requirements.
- **Security Management**. The TOE provides administrative interfaces that permit users with administrative profiles to configure and manage the TOE. This includes management of the attributes used in the Administrative Access Control Security Functional Policy (SFP), and device management. Additionally, administrator roles are provided with differing privileges.
- **Protection of the TSF.** Confidentiality is provided when policy information is transferred from the TOE to the managed devices. Reliable time stamps are provided in support of the audit function.
- **Trusted Path/Channel**. The TOE requires an encrypted trusted channel for communication between the TOE and the managed devices in support of the transfer of policy information. A trusted path communication is required in support of remote administration.

PHYSICAL ARCHITECTURE

The TOE is the firmware "Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)", running in stand-alone 'FIPS-CC' mode, that can be deployed in seven different hardware devices, deriving in the following firmware instances:

- FMG-400E-v5.6.6-build7352-FORTINET.out
- FMG-1000D-v5.6.6-build7352-FORTINET.out
- FMG-2000E-v5.6.6-build7352-FORTINET.out
- FMG-3000F-v5.6.6-build7352-FORTINET.out
- FMG-3900E-v5.6.6-build7352-FORTINET.out
- FMG-4000D-v5.6.6-build7352-FORTINET.out
- FMG-4000E-v5.6.6-build7352-FORTINET.out

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- FortiManager 5.6.6 Administration Guide, November 22, 2018, 02-566-400706-20181122 (available in Portable Document Format (pdf) as FortiManager-5.6.6-Administration-Guide.pdf).
- FortiManager 5.6.6 CLI Reference, November 15, 2018, 02-566-400067-20181115 (available in pdf as FortiManager 5.6.6 CLI Reference.pdf).
- FortiManager & FortiAnalyzer 5.6.6 Event Log Reference, October 02, 2018, 05-566-438656-20181002 (available in pdf as FMG-FAZ 5.6.6 Event Log Reference.pdf).
- FortiManager 5.6.6 Common Criteria EAL4 Technote, June 12, 2019, 02-566-486071-20190604 (available in pdf as FMG 5.6.6 CC EAL4 Technote.pdf).

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the laboratory premises. In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product “Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)” it is necessary the disposition of the following elements:

Non-TOE Component	Hardware/Software Requirements
FortiManager Appliance	Any of the following hardware models may be used with theTOE: • FMG-400E • FMG-1000D • FMG-2000E • FMG-3000F • FMG-3900E • FMG-4000D • FMG-4000E
Management Workstation	General purpose computing platform that supports the following: • Internet Explorer 11 • Transport Layer Security (TLS) 1.1 or 1.2
Fortinet Entropy Token	Fortinet Entropy Token hardware
Managed Devices	Fortinet FortiGate and FortiAnalyzer devices

EVALUATION RESULTS

The product "Fortinet FortiManager 5.6.6 build 7352 190510 (EAL4+)" has been evaluated against the Security Target Fortinet FortiManager 5.6.6 Security Target v1.13 (21 October 2019).

All the assurance components required by the evaluation level EAL4 + ALC_FLR.3 have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4 + ALC_FLR.3, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- There is no additional recommendation from the Laboratory in order to use the TOE since guidance documentation is enough to make a secure usage of the TOE.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Applus Laboratories, a positive resolution is proposed.

- There is no additional recommendation from the Certification Body.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[ST] Fortinet FortiManager 5.6.6 Security Target v1.13 (21 October 2019).

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: Fortinet FortiManager 5.6.6 Security Target v1.13 (21 October 2019).

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.