TÜV Rheinland Nederland B.V.

Certification Report

Huawei FusionDirector version 1.5.1.SPC1

Sponsor and developer: ***Huawei Technologies Co.,Ltd.***
D4 Building, Southern Factory,
Songshanhu,
Dongguan,
China

Evaluation facility: ***Riscure***
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-0115712-CR**
Report version:	**1**
Project number:	**0115712**
Author(s):	**Denise Cater**
Date:	**12 June 2020**
Number of pages:	**11**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, 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 or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Huawei FusionDirector version 1.5.1.SPC1. The developer of the Huawei FusionDirector version 1.5.1.SPC1 is Huawei Technologies Co.,Ltd. located in Dongguan, China and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

Huawei FusionDirector enables unified server hardware operation and maintenance (O&M). Public cloud and enterprise users can use FusionDirector to perform simple and efficient O&M for Huawei servers in each phase of the life cycle.

FusionDirector implements visualized management and fault diagnosis for servers, and provides lifecycle management capabilities such as device management, device configuration, firmware upgrade, device monitoring, and OS deployment for Huawei servers.

FusionDirector can be widely used in Huawei public cloud, private cloud, data center, carrier, and enterprise customers. It can be deployed in multiple scenarios such as AI, HPC, Internet, and Safe City.

The TOE consists of micro-services deployed on a supporting Guest OS (Euler OS) which also provides elementary Linux operating system security mechanisms that contribute the enforcements of SFRs. The TOE is to be deployed on a virtualization environment running on server hardware which are not in the scope of the evaluation.

The main security service provided by the TOE is the protection of the remote management interfaces including communication security, authentication and authorization access controls, and the audit/logging of security relevant events.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 12 June 2020 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Huawei FusionDirector version 1.5.1.SPC1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Huawei FusionDirector version 1.5.1.SPC1 are advised to verify that their own environment is consistent with 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 provides sufficient evidence that the TOE meets the EAL2 assurance requirements for the evaluated security functionality.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Huawei FusionDirector version 1.5.1.SPC1 from Huawei Technologies Co.,Ltd. located in Dongguan, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Huawei FusionDirector 1.5.1.SPC1	1.5.1.SPC1

To ensure secure usage a set of guidance documents is provided together with the Huawei FusionDirector version 1.5.1.SPC1. Details can be found in section 2.5 of this report.

2.2 Security Policy

The TOE provides all the following main security features:

- Authentication
- Authorization
- Access Control
- Auditing
- Communication Security
- Cryptographic Functions
- Software Integrity Protection

The communication is based on the following protocols:

- SSHv2: provided by Euler OS
- SFTP: provided by Euler OS
- NTP: provided by Euler OS
- NFS: provided by Euler OS
- HTTPS(TLS1.1/1.2): provided by Nginx in FusionDirector
- Docker VXLAN (Overlay) : provided by Docker Engine

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

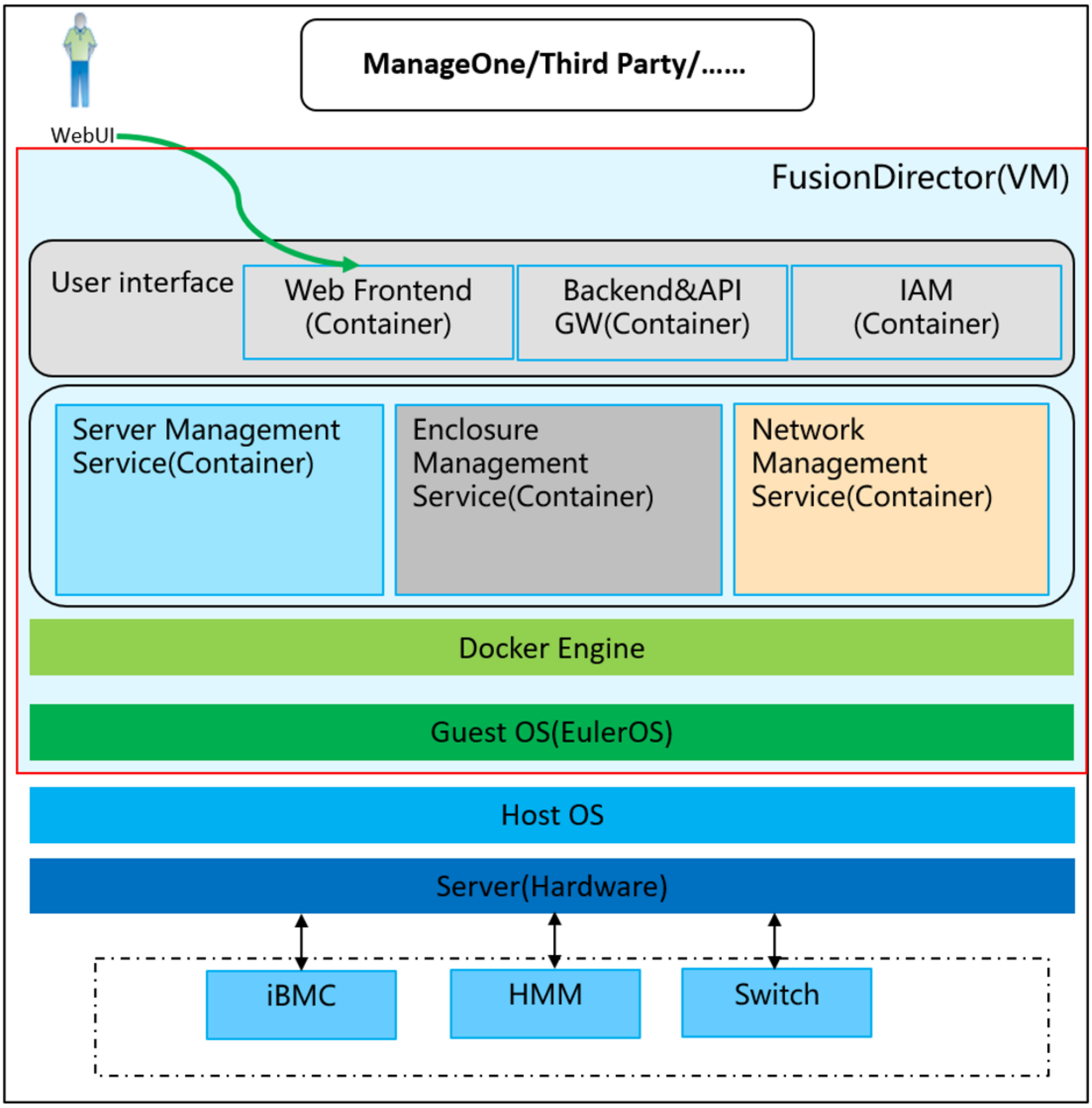
2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

As detailed in *[ST]* section 1.3.2, the Host OS of virtual machine and the underlying hardware server are not in the scope of the TOE.

2.4 Architectural Information

The TOE consists of FusionDirector software and Euler OS (see red box in the figure). The Guest OS is Euler OS, version is EulerOS V200R007C00SPC516 used by TOE. The SSH, SFTP, NTP, NFS server used by the TOE is provided by Euler OS.



In terms of the software, the TOE's software architecture consists of one logical plane to support centralized management mechanism.

FusionDirector belongs to server management software, it mainly implements server status monitoring, configuration, firmware upgrade and OS deployment functions. FusionDirector uses micro-service architecture, provides Restful API to the outside world, and uses reverse proxy to listen for external requests. All external messages are forwarded to API gateway by reverse proxy. API gateway realizes authentication and authorization of external messages through interaction with Identity and Access Management (IAM) micro-service. After authentication and authorization, the message is forwarded to the target micro-service for processing.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Huawei FusionDirector 1.5.1.SPC1 -AGD_PRE_User	V5.0
Huawei FusionDirector 1.5.1.SPC1- AGD_OPE	V4.1
OpenPGP Signature Verification Guide	04
FusionDirector Installation Guide 01	01
FusionDirector Operation Guide	02

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer devised 32 test cases providing evidence of coverage for the security functionality. The evaluator sampled the two most complex of these developer tests.

In addition, the evaluator devised three additional independent evaluator tests to further complement the coverage.

2.6.2 Independent Penetration Testing

The TOE is a web-server based solution. Therefore, the vulnerability analysis is conducted using the network attack methods, and is structured in the following phases:

- Information Gathering and Potential Vulnerability Identification: understand network structures, server properties using port scanning, detection of running services etc. and conducting public vulnerability searches to identify potential vulnerabilities
- Exploitation: get some first unprivileged access e.g. by manipulating file upload mechanisms, SQL injections, password attacks, cross-site scripting etc.
- Privilege escalation: escalate to extended / root privileges to gather further information on operating system properties, application services, file-system structures to get deeper into the system and break security features

The vulnerability analysis takes information from the design assessment of the TOE into account. However, an EAL2 evaluation is more explorative in nature than a full white-box evaluation where also implementation details and source code is available for inspection, so specific emphasis is placed upon the information gathering activities.

Overall the evaluator devised and four logical verification and penetration tests, one of which was an in-depth scan and assessment of the Web-UI that forms the primary exposed attack surface. The tests efforts accumulated to 10 days.

2.6.3 Test Configuration

The penetration testing was performed on a remotely accessible test instance of the product that was configured according to the default configuration of Huawei FusionDirector 1.5.1.SPC1 as supplied also to the customer. The installation for the independent testing was hosted on a VMware ESXi virtualization platform (HostOS).

The evaluator had full administrator access to facilitate an efficient in-depth inspection of the system.

The testing was performed using a extensive network and web-server penetration testing toolbox consisting of standard tools with laboratory maintained extensions.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e. from the current best cryptanalytic attacks published, has been taken into account.

2.7 Re-used evaluation results

There is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei FusionDirector version 1.5.1.SPC1.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Huawei FusionDirector version 1.5.1.SPC1, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE.

From the recommendations and obligations detailed in the TOE user guidance documents, are the requirements that the TOE needs to be operated in a segregated network that only allows for access via the remote interfaces and by physically protected (OE.NetworkSegration and OE.PhysicalProtection).

For further details the user shall refer to *[ST]* and to the guidance documentation as listed in section 2.5 above.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

3 Security Target

The Huawei FusionDirector 1.5.1.SPC1 Security Target, V2.1, 2020-06-04 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
TOE	Target of Evaluation
VLAN	Virtual LAN

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[ETR] Evaluation Technical Report for Huawei FusionDirector 1.5.1.SPC1, 20190576-D3, Version 1.2, 11 June 2020.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[ST] Huawei FusionDirector 1.5.1.SPC1 Security Target, V2.1, 2020-06-04.

(This is the end of this report).