Reference: 2023-10-INF-4497- v1
Target: Limitada al expediente
Date: 14.04.2025

Created by: I007
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2023-10**
TOE	**Huawei EulerOS 2.0 (V200R011C00 patch version SPC501)**
Applicant	**914403001922038216 - Huawei Technologies Co.,Ltd.**
References	
	[EXT-8419] Certification Request
	[EXT-9410] Evaluation Technical Report

Certification report of the product Huawei EulerOS 2.0 (V200R011C00 patch version SPC501), as requested in [EXT-8419] dated 09/03/2023, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9410] received on 20/12/2024.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei EulerOS 2.0 (V200R011C00 patch version SPC501).

Huawei EulerOS 2.0 (V200R011C00 patch version SPC501) is a highly-configurable Linux-based general-purpose operating system, which has been developed to provide a good level of security as required in commercial environments.

Developer/manufacturer: Huawei Technologies Co.,Ltd.

Sponsor: Huawei Technologies Co.,Ltd..

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

ITSEF: Applus Laboratories.

Protection Profile: Operating System Protection Profile, BSI-CC-PP-0067, Version 2.0, 2010-06-01.

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

Evaluation end date: 16/01/2025.

Expiration Date[1]: 26/03/2030

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 Huawei EulerOS 2.0 (V200R011C00 patch version SPC501), a positive resolution is proposed.

TOE SUMMARY

Huawei EulerOS 2.0 is a general purpose, multi-user, multi-tasking Linux based operating system. It provides a platform for a variety of applications, including services on cloud environment.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

Huawei EulerOS 2.0 evaluation covers a potentially distributed network of systems running the evaluated version and its configurations as well as other peer systems operating within the same management domain. The hardware platforms selected for the evaluation consist of machines that are available on market when the evaluation has completed and to remain available for a substantial period of time afterwards.

The TOE Security Functions (TSFs) consist of functions of Huawei EulerOS 2.0 that run in kernel mode plus some trusted processes running in user mode. These are the functions that enforce the security policy as defined in the Security Target. Tools and commands executed in user mode that are used by an administrative user need also to be trusted to manage the system in a secure way, but they are not considered to be part of the TSF, just as with other operating system evaluations.

The hardware, BIOS firmware and potentially other firmware layers between the hardware and the TOE, are considered to be part of the TOE environment.

The TOE includes standard networking applications, such as sshd(8), which allow to access the TOE via cryptographically protected communication channel.

System administration tools include the standard command line tools. A graphical user interface for system administration or any other operation is not included in the evaluated configuration.

The TOE environment also includes applications that are not evaluated, but are used as unprivileged tools to access public system services. For example, a network server using a port above 1024 may be used as a normal application running without root privileges on top of the TOE. Additional documentation is available that provides guidance how to set up such applications on the TOE in a secure way.

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 to the table, 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_LCD.1
	ALC_TAT.1
	ALC_FLR.3
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	FCS_CKM.4	FIA_AFL.1	FMT_MSA.3(TSO)	FMT_REV.1(USR)
FAU_GEN.2	FCS_COP.1(NET)	FIA_ATD.1(HU)	FMT_MSA.3(NI)	FMT_SMF.1
FAU_SAR.1	FCS_RNG.1(SSL-DFLT)	FIA_ATD.1(TU)	FMT_MSA.4(PSO)	FMT_SMR.1
FAU_SAR.2	FDP_ACC.1(PSO)	FIA_SOS.1	FMT_MTD.1(AE)	FPT_STM.1
FAU_SEL.1	FDP_ACC.1(TSO)	FIA_UAU.1	FMT_MTD.1(AS)	FPT_TDC.1
FAU_STG.1	FDP_ACF.1(PSO)	FIA_UAU.5	FMT_MTD.1(AT)	FTA_SSL.1
FAU_STG.3	FDP_ACF.1(TSO)	FIA_UAU.7	FMT_MTD.1(AF)	FTA_SSL.2
FAU_STG.4	FDP_IFC.2(NI)	FIA_UID.1	FMT_MTD.1(NI)	FTP_ITC.1
FCS_CKM.1(SYM)	FDP_IFF.1(NI)	FIA_USB.2	FMT_MTD.1(IAT)	
FCS_CKM.1(RSA)	FDP_ITC.2	FMT_MSA.1(PSO)	FMT_MTD.1(IAF)	
FCS_CKM.1(ECDSA)	FDP_RIP.2	FMT_MSA.1(TSO)	FMT_MTD.1(IAU)	
FCS_CKM.2(NET)	FDP_RIP.3	FMT_MSA.3(PSO)	FMT_REV.1(OBJ)	

IDENTIFICATION

Product: Huawei EulerOS 2.0 (V200R011C00 patch version SPC501)

Security Target: EulerOS 2.0 Security Target, Version 1.6, 2024-10-29.

Protection Profile: Operating System Protection Profile, BSI-CC-PP-0067, Version 2.0, 2010-06-01.

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

SECURITY POLICIES

The use of the product Huawei EulerOS 2.0 (V200R011C00 patch version SPC501) shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3.2 ("Organizational Security Policies").

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following 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.

The detail of these assumptions is documented in the Security Target, section 3.3 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei EulerOS 2.0 (V200R011C00 patch version SPC501), although the agents implementing attacks have the attack potential according to the Enhanced-Basic of EAL4 augmented with 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.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3.1 ("Threats").

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 those defined in the Protection Profile and they are documented in the Security Target, section 4.2 ("Security Objectives for the Operational Environment").

ARCHITECTURE

LOGICAL ARCHITECTURE

The primary security features of the TOE include:

- Cryptographic communication: The TOE provides cryptographically secured communication to allow remote entities to log into the TOE. The SSHv2 protocol is provided to set up interactive session with the TOE. The TOE provides both the server side and the client side applications. Using the OpenSSH suite, password-based and public-key-based authentication are allowed.
- The TOE implements TLS protocol to enable a trusted network channel that is used for client and server authentication. It is used in HTTPS service.
- Packet filter: The TOE kernel implements layering structure of network protocols. It has IPTables mechanism to provide a stateful packet filter at network layer and transfer layer for regular IP-based communication. Ethernet frames routed through bridges are controlled by a lower-layer packet filter, EBTables, which is not covered in this evaluation.
- Identification and Authentication: User identification and authentication in the TOE includes all forms of interactive login (e.g. using the SSH protocol or log in at the local console) as well as identity changes through the command like su or sudo. These all rely on explicit authentication information provided interactively by a user.
- The authentication security function allows password-based authentication. For SSH access, public-key-based authentication is also supported.
- Password quality enforcement mechanisms offered by the TOE are enforced at the time when the password is changed.
- Discretionary Access Control (DAC): DAC allows owners of named objects to control the access permissions to these objects. The owners can permit or deny access by other users based on the configured permission settings. The DAC mechanism is also used to ensure that untrusted users cannot tamper with the TOE mechanisms.
- Auditing: The Lightweight Audit Framework (LAF) is designed to be an audit system making Huawei EulerOS 2.0 compliant with the requirements from Common Criteria. LAF is able to intercept all system calls as well as retrieving audit log entries from privileged user space applications. The subsystem allows to configure the events to be actually audited from the

set of all events that are possible to be audited, and to review and search audit logs retrieved.

- Security Management: The security management facilities provided by the TOE are usable by authorized users and/or authorized administrators to modify the configuration of TSF. The TOE allows local management on local consoles and remote management via OpenSSH. Administrative users can log in remotely and perform the same management tasks as a locally operating administrator.

PHYSICAL ARCHITECTURE

The TOE EulerOS-V2.0SP11-x86_64-dvd.iso (version V200R011C00, a.k.a 2.0) is supplied in the form of ISO images distributed via the Huawei Network.

The patch package CVE-Fixed-Packages-SPC501.zip is sent to the end user via email in the form of archive.

DOCUMENTS

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

The following documentations are provided for the TOE and delivered by email:

- Installation guide: EulerOS2.0_AGD_PRE, delivered in *docx* format.
- User guide: EulerOS2.0_AGD_OPE, delivered in *docx* format.
- Man pages: EulerOS2.0_MAN_PAGES delivered in *zip* format.
- Patch package: CVE-Fixed-Packages-SPC501 delivered in *zip* format.

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 developer 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.

Through the tests performed by the Laboratory it is concluded that 100% of the SFRs and all the TSFIs defined in the Functional Specification has been tested.

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment, the evaluation team has devised attack scenarios for penetration tests. Within these activities all aspects of the security architecture which were not covered by functional testing have been considered. The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Enhanced-Basic has been successful in the TOE's operational environment as defined in the security target when all security measures required by the developer in the security guidance defined in DOCUMENTS section are applied.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Huawei EulerOS 2.0 (V200R011C00 patch version SPC501) it is necessary the disposition of one of the following physical platforms:

According to the Security Target, section 1.3.3 ("Non-TOE Hardware, Software, Firmware supported"), the following physical and virtual hardware platforms, corresponding firmware, and components are supported by the TOE:

- Huawei TaiShan 2280E, 2280, 2180, 2480
- Huawei TaiShan 5280, 5290
- Huawei TaiShan 1280
- Huawei TaiShan X6000, XA320
- Atlas 500 Pro Model 3000
- OceanStorDorado 6000 V6
- OceanStorDorado 5000 V6
- OceanStorPacific 9520
- Atlas 800 9000

- Atlas 800D G1
- PoweLeader BD-21083F3
- FusionServer 1288H V5 V6 V7
- FusionServer 2288H V3 V4 V5 V6 V7
- FusionServer 2288 V3 V4 V5 V6 V7
- FusionServer 5288 V5 V6 V7
- FusionServer 2298 V5
- FusionServer 2488 V5
- FusionServer 2488H V5 V6 V7
- FusionServer 5885H V5 V6 V7
- KunLun 9008 V5

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is the following:

- **FusionServer RH2288H V3 Rack Server, BIOS V515**.

The evaluated configuration is defined as follows:

- The package set evaluated by CC for the TOE must be selected at install time according to the installation guide and be installed accordingly.
- The TOE supports the use of IPv4 and IPv6, both are also supported in the evaluated configuration.
- The default configuration for identification and authentication include both the defined password-based PAM modules and the key-based authentication for OpenSSH. Support for other authentication options, e.g. smart card authentication, is not included in the evaluation configuration.
- If the system console is used, it must be connected directly to the TOE and afforded the same physical protection as the TOE.
- The TOE shall run in the “Normal mode” of operation.

Configurations and settings that are different from that specified in the installation guide are not permitted.

EVALUATION RESULTS

The product Huawei EulerOS 2.0 (V200R011C00 patch version SPC501) has been evaluated against the Security Target *EulerOS 2.0 Security Target, Version 1.6, 2024-10-29*.

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 for Information Technology Security Evaluation v3.1 R5 and the [CEM] Common Methodology for Information Technology Security Evaluation 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.

- To follow the security guidance's of the TOE strictly.
- To keep the TOE under personal control and set all other security measures available from the environment.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei EulerOS 2.0 (V200R011C00 patch version SPC501), a positive resolution is proposed.

As the Security Target states, it is recommended to upgrade the firmware to the latest version to avoid the impact of known vulnerabilities. Particularly, it is important to note that the BIOS version for the physical platform evaluated as operational environment (FusionServer RH2288H V3 Rack Server) must be V515 or higher.

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

https://oc.ccn.cni.es
organismo.certificacion@cni.es

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.

[PP] Operating System Protection Profile, BSI-CC-PP-0067, Version 2.0, 2010-06-01.

[ST] EulerOS 2.0 Security Target, Version 1.6, 2024-10-29.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- EulerOS 2.0 Security Target, Version 1.6, 2024-10-29.

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.eu.

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.