Reference: 2018-2-INF-2787-v1
Target: Público
Date: 28.05.2019

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2018-2**
TOE	**Huawei EulerOS v2.0**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**
References	

[EXT-3741] 2018-02 Solicitud de Certificación

Certification report of the product Huawei EulerOS v2.0, as requested in [EXT-3741] dated 15/01/2018, and evaluated by Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-3741] received on 16/05/2019.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei EulerOS v2.0.

EulerOS 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.

The TOE Security Functions (TSFs) consist of functions of EulerOS 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 this 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 this TSF, just as with other operating system evaluations.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd..

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

ITSEF: Epoche and Espri, S.L.U.

Protection Profile:

- Common Criteria Protection Profile, BSI-CC-PP-0067, Version 2.0; strict conformance;
- OSPP Extended Package - Trusted Boot, BSI-CC-PP-0067, OSPP EP-TB, Version 2.0; strict conformance;
- OSPP Extended Package - Integrity Verification, BSI-CC-PP-0067, OSPP EP-IV, Version 2.0; strict conformance;
- OSPP Extended Package - Advanced Management, BSI-CC-PP-0067, OSPP EP-AM, Version 2.0; strict conformance;

Evaluation Level: Common Criteria v3.1 r5 – EAL4 + ALC_FLR.3.

Evaluation end date: 16/05/2019.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.3) have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4, 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 v2.0, a positive resolution is proposed.

TOE SUMMARY

EulerOS 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.

EulerOS provides the following key security features:

- Security Audit: The TOE is able to intercept all system calls and recording the events occurred in the system. The security audit functionality also allows to configure the events to be audited, review and search the audit log retrieved.
- Cryptographic support: The TOE provides cryptographically secured communication to allow remote entities to log into the TOE. It is achieved by using the SSHv2 protocol. The TOE also provided IPSec and TLS protocols in order to secure the communications with other IT entities. Moreover, the TOE offers the possibility of encrypt stored data.
- Identification and Authentication: The TOE includes several ways to identify and authenticate the users (via the local console using username and password or via the SSH using password and public-key based authentication. The TOE also offers a password quality enforcement mechanism as well as it is able to handle failed authentication attempts.
- User Data Protection: The TOE offers a Discretionary Access Control (DAC) which allow owner of named objects to control the access permissions to these objects. Moreover, the TOE kernel implements the IPTables mechanism in order to provide a packet filter at network and transfer layer. Using these two mechanism the TOE offers an access control policy as well as an information flow control policy.
- Security Management: The TOE offers to the users and/or authorized administrators the possibility of modifying the configuration of TSF. The TOE allows local and remote management using by using OpenSSH.
- Protection of the TSF: The TOE has a boot and system integrity verification mechanisms which assure that any attempt to compromise the integrity of the TOE is detected. This is achieved by signed the kernel image together with its modules. Moreover, sensitive files stored in the user space are protected using IMA appraisal.
- TOE Access: The TOE is able to end user sessions after an inactivity period of time. This can be initiated by the TSF itself or by user request.
- Trusted Channel: Using the cryptographic communication protocols above mentioned (SSH, IPSec and TLS) the TOE is able to establish secure and trusted communication channel with other IT entities.

These primary security features are supported by domain separation and reference mediation, which can ensure that the security features are always invoked and cannot be bypassed.

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 components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.3 Systematic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 r5:

FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association

FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SEL.1	Selective audit
FAU_STG.1	Protected audit trail storage
FAU_STG.3	Action in case of possible audit data loss
FAU_STG.4	Prevention of audit data loss
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FCS_RNG.1	Random number generation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.2	Complete information flow control
FDP_IFF.1	Simple security attributes
FDP_ITC.2	Import of user data with security attributes
FDP_RIP.2	Full residual information protection
FDP_RIP.3	Full residual information protection of resources
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.7	Protected authentication feedback
FIA_UID.1	Timing of identification
FIA_USB.2	Enhanced user-subject binding
FMT_MSA.1	Management of object security attributes
FMT_MSA.3	Static attribute initialization
FMT_MSA.4	Security attribute value inheritance
FMT_MTD.1	Management of TSF data
FMT_REV.1	Revocation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps
FPT_TDC.1	Inter-TSF basic TSF data consistency
FTA_SSL.1	TSF-initiated session locking
FTA_SSL.2	User-initiated locking
FTP_ITC.1	Inter-TSF trusted channel
FMT_SMR.2	Restrictions on security roles
FPT_TIM.1	TSF integrity monitoring and action
FDP_SDI.2	Stored data integrity monitoring and action

IDENTIFICATION

Product: Huawei EulerOS v2.0

Security Target: EulerOS 2.0 Security Target, version 0.13, 13/04/2019

Protection Profile:

- Common Criteria Protection Profile, BSI-CC-PP-0067, Version 2.0; strict conformance;
- OSPP Extended Package - Trusted Boot, BSI-CC-PP-0067, OSPP EP-TB, Version 2.0; strict conformance;
- OSPP Extended Package - Integrity Verification, BSI-CC-PP-0067, OSPP EP-IV, Version 2.0; strict conformance;
- OSPP Extended Package - Advanced Management, BSI-CC-PP-0067, OSPP EP-AM, Version 2.0; strict conformance;

Evaluation Level: Common Criteria v3.1 r5 – EAL4 + ALC_FLR.3.

SECURITY POLICIES

The use of the product Huawei EulerOS v2.0 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 (Organisational 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 Huawei EulerOS v2.0, although the agents implementing attacks have the attack potential according to the Enhanced Basic of EAL4 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).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE is described in title 1.4.2.2 in [ST].

The TOE includes the following functional sections:

- Cryptographic communication
- Packet filter
- Encrypted data storage
- Identification and Authentication
- Discretionary Access Control (DAC)
- Auditing
- Security Management
- Boot integrity and system integrity

PHYSICAL ARCHITECTURE

The TOE is supplied in the form of ISO images distributed via the Huawei Network.

- Download URL: https://developer.huawei.com/ict/cn/rescenter/CMDA_FIELD_EULER_OS
- Filename: EulerOS-V2.0-x86_64-dvd.iso
- Hash (SHA-256): 6339201bd2505e3a5e7e631937575e09b6e897ea585209b84a2548c438a8f967

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

- Installation guide: Huawei EulerOS V2.0 Installation Guide v0.6, delivered in .pdf format

- User guide: Huawei EulerOS V2.0 User Guide v0.6, delivered in .pdf format

The list of hardware applicable to the TOE is given above. The analysis of the hardware capabilities as well as the firmware functionality is covered by this evaluation to the extent that the following capabilities supporting the security functionality are analyzed and tested:

- Memory separation capability
- Unavailability of privileged processor states to untrusted user code
- Full testing of the security functionality on all hardware systems given above

DOCUMENTS

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

- Huawei EulerOS2.0 V2.0 User Guide v0.6, version 0.6, April 28, 2019.
- Huawei EulerOS2.0 V2.0 Installation Guide v0.6, version 0.6, April 28, 2019.

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 a sample of the developer functional tests in the developer premises.

The evaluator considered that the TSFIs and subsystems tests defined by the developer are correct having checked that the results obtained when repeating the tests are the same than the results obtained by the developer.

EVALUATED CONFIGURATION

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals (see *DOCUMENTS* section of this certification report.

EVALUATION RESULTS

The product Huawei EulerOS v2.0 has been evaluated against the Security Target EulerOS 2.0 Security Target, version 0.13, 13/04/2019.

All the assurance components required by the evaluation level EAL4 + ALC_FLR.3 have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. 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.

- It is mandatory to strictly follow the steps indicated in the installation documentation in order to download and install the correct version of the TOE in a proper manner.
- The user guidance must be read and understood in order to operate the TOE in an adequate manner according to the security target.

CERTIFIER RECOMMENDATIONS

In order to download and install the evaluated version of the TOE, the below information is given:

- Download URL: https://developer.huawei.com/ict/cn/rescenter/CMDA_FIELD_EULER_OS
- Filename: EulerOS-V2.0-x86_64-dvd.iso
- Hash (SHA-256): 6339201bd2505e3a5e7e631937575e09b6e897ea585209b84a2548c438a8f967

Although several versions can be found in the provided Download URL link, only the V2.0 one with the provided hash has been evaluated and therefore covered by this certification report.

Considering the obtained evidences during the instruction of the certification request of the product Epoche & Espri S.L.U., a positive resolution is proposed.

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.

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 0.13, 13/04/2019.

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 assurance components up to EAL4.

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.