REF: 2017-22-INF-2257v1	Created by: CERT10
Target: Público	Revised by: CALIDAD
Date: 08.03.2018	Approved by: TECNICO

CERTIFICATION REPORT

File: 2017-22 EulerOS v2.0 build 3.10.0-327.59.59.46.h34.x86_64

Applicant: Huawei Technologies Co., Ltd.

References:

[EXT-3407] Certification request of EulerOS v2.0

[EXT-3780] Evaluation Technical Report of EulerOS v2.0.

The product documentation referenced in the above documents.

Certification report of EulerOS v2.0 build 3.10.0-327.59.59.46.h34.x86_64, as requested in [EXT-3407] on 07/06/2017, and evaluated by Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-3780] received on 28/12/2017.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product EulerOS v2.0 build 3.10.0-327.59.59.46.h34.x86_64.

The TOE, EulerOS v2.0 build 3.10.0-327.59.59.46.h34.x86_64, is a general-purpose, multi-user and multi-tasking Linux- based operating system. It provides a platform for a variety of applications, including services for cloud environments.

The TOE evaluation has covered 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 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.

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

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 & Espri S.L.U.

Protection Profile: NIAP - Protection Profile for General Purpose Operating Systems, Version: 4.1 [GPOSPP]

Evaluation Level: Common Criteria v3.1 R5 (assurance packages according to the [GPOSPP]).

Evaluation end date: 28/12/2017.

All the assurance components required by the [GPOSPP] 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 [GPOSPP] assurance level packages, as defined by the Common Criteria v3.1 R5, the [GPOSPP] and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product EulerOS v2.0 build 3.10.0-327.59.59.46.h34.x86_64, a positive resolution is proposed.

TOE SUMMARY

The TOE performs the following security functions:

1) Cryptographic Support

The TOE offers different cryptographic services in kernel, and provides a socket interface to user space applications. In addition, it also provides cryptographic algorithms for general use in user space.

As a summary, these cryptographic services have been analyzed as part of the evaluation. EulerOS...

● uses the Cryptographic Algorithm and its Standards.

● overwrites critical cryptographic keys at garbage collection time.

● provides crypto APIs (eg, openssl library) for developers and the cryptsetup tool for system administrators to encrypt and decrypt sensitive data.

● implements TLS to provide server and mutual authentication, confidentiality and integrity to upper layer protocols such as Extensible Authentication Protocol and HTTPS.

● implements SSHv2 to provide security network communication channel.

2) User Data Protection

The general security policy determines that subjects (i.e., processes) are allowed only the accesses specified by the policies applicable to the object the subject requests access to. Further, the ability to propagate access permissions is limited to those subjects who have that permission, as determined by the policies applicable to the object the subject requests access to. EulerOS does not provide a VPN client; however, it provides related APIs in package libreswan, which can be used to enable VPN clients to protect IP traffic using the IPsec tunneling protocol.

3) Security Management

The following table lists which activities can be done by a EulerOS user or a local administrator. A checkmark indicates which entity can invoke the management function. General users, or programs running on their behalf, are not able to modify policy or configuration that is set by the privileged administrator, which results in that the user cannot override the configuration specified by the administrator. EulerOS provides the user with the capability to administer the security functions described in the security target. The mappings to specific functions are described in each applicable section of the TOE Summary Specification.

4) Protection of the TSF

The TSF provides a security domain for its own protection and provides process isolation. The security domains used within and by the TSF consists of the following components:

- Hardware
- Kernel-mode software
- Trusted user-mode processes
- User-mode Administrative tools process

The TSF hardware is managed by the TSF kernel-mode software and is not modifiable by untrusted subjects. The TSF kernel-mode software is protected (from read and write) by hardware execution state. The TSF provides process isolation for all user-mode processes through private virtual address spaces (private process page tables), execution context (registers, program counters, resource usage registrations), and security context (process credentials, capabilities, control group information, security attributes). User-mode administrator tools execute with the security context of the process running on behalf of the authorized administrator. Administrator processes are also protected like other user-mode processes, by process isolation.

5) Audit

The Lightweight Audit Framework (LAF) is used in the audit subsystem of EulerOS, which is compliant with the requirements from Common Criteria. The EulerOS kernel implements the core of the LAF functionality. It gathers all audit events, analyzes these events based on the audit rules, collects related information, and forwards the audit events that are requested to be audited to the audit daemon executing in user space. The audit functionality of the Linux kernel is controlled by an audit management tool in user space, which communicates with the kernel through a specific netlink channel. This netlink channel is usable only by applications with the following capabilities:

- Performing management operations like adding or deleting audit rules, setting or getting auditing parameters;
- Submitting audit records to the kernel which in turn forwards the audit records to the audit daemon.

The TOE Audit security functionality includes:

- Audit event selection
- Audit trail
- Audit log overflow protection
- Audit log access protection

6) Identification and Authentication

Each user trying to access a EulerOS instance must have an account on the system. To authenticate a user account, a password is set for it and is saved by EulerOS after encryption. All logons are treated essentially in the same manner regardless of

their forms (e.g., log in remotely using the SSH protocol, log in at the local console) and start with an account name and credentials that must be provided to the TSF.

For a remote login through the OpenSSH server, the administrator is allowed to enable SSH key-based authentication in addition or instead of the username/password based authentication. When a user can successfully authenticate using the SSH key-based authentication based on a private SSH key in his possession, the TOE grants the user access.

7) Trusted Path/Channels

EulerOS provides trusted network channels to communicate with supporting IT infrastructure or applications:

● Using TLS (HTTPS) for certificate enrolment; CRL checking; authentication to network resources such as web (HTTPS).

● SSH is for user log in.

EulerOS provides trusted network channels, which protect data in transit from disclosure, provide data integrity and endpoint identification that is used by TLS, HTTPS and SSH for network-based authentication and certification validation.

EulerOS provide a local trusted path service using SAK and a network-based trusted channel built on the network protocols described in this section.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidences required to fulfil the assurance packages defined in [GPOSPP], according to Common Criteria v3.1 R5.

Class	Family/Component
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.1 Security objectives ASE_REQ.1 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labeling of the TOE ALC_CMS.1 TOE CM Coverage ALC_TSU_EXT.1 Timely Security Updates
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.1 Independent Testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability Survey

SECURITY FUNCTIONAL REQUIREMENTS

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

Requirement Class	Requirement Component
Security Audit (FAU)	Audit Data Generation (FAU_GEN.1)
Cryptographic Support (FCS)	Cryptographic Key Generation for (FCS_CKM.1(1))
	Cryptographic Key Establishment (FCS_CKM.2(1)
	Cryptographic Key Destruction (FCS_CKM_EXT.3)
	Cryptographic Operation for Data Encryption/Decryption (FCS_COP.1(SYM))
	Cryptographic Operation for Hashing (FCS_COP.1(HASH))
	Cryptographic Operation for Signing (FCS_COP.1(SIGN))
	Cryptographic Operation for Keyed Hash Algorithms (FCS_COP.1(HMAC))
	Random Bit Generation (FCS_RBG_EXT.1)
	Storage of Sensitive Data (FCS_STO_EXT.1)
	TLS Client Protocol (FCS_TLSC_EXT.1)
	TLS Client Protocol (FCS_TLSC_EXT.2)
	TLS Client Protocol (FCS_TLSC_EXT.3)
	TLS Client Protocol (FCS_TLSC_EXT.4)
	DTLS Implementation (FCS_DTLS_EXT.1)
User Data Protection (FDP)	Access Controls for Protecting User Data (FDP_ACF_EXT.1)
	Information Flow Control (FDP_IFC_EXT.1)
Identification & Authentication (FIA)	Authorization Failure Handling (FIA_AFL.1)
	Multiple Authentication Mechanisms (FIA_UAU.5)
	X.509 Certification Validation (FIA_X509_EXT.1)
	X.509 Certificate Authentication (FIA_X509_EXT.2)
Security Management (FMT)	Management of Security Functions Behavior (FMT_MOF_EXT.1)
Protection of the TSF (FPT)	Access Controls (FPT_ACF_EXT.1)
	Address Space Layout Randomization (FPT_ASLR_EXT.1)
	Stack Buffer Overflow Protection (FPT_SBOP_EXT.1)
	Software Restriction Policies (FPT_SRP_EXT.1)
	Boot Integrity (FPT_TST_EXT.1)
	Trusted Update (FPT_TUD_EXT.1)
	Trusted Update for Application Software (FPT_TUD_EXT.2)
TOE Access (FTA)	Default TOE Access Banners (FTA_TAB.1)
Trusted Path/Channels (FTP)	Trusted Path (FTP_TRP.1)
	Trusted Channel Communication (FTP_ITC_EXT.1(TLS))
	Trusted Channel Communication (FTP_ITC_EXT.1(DTLS))

IDENTIFICATION

Product: EulerOS v2.0 build 3.10.0-327.59.59.46.h34.x86_64

Security Target: EulerOS 2.0 Security Target. Version 0.9. 2017-12-20.

Protection Profile: NIAP - Protection Profile for General Purpose Operating Systems, Version: 4.1, 2016-03-09 [GPOSPP].

Evaluation Level: Common Criteria v3.1 R5 (assurance packages according to the [GPOSPP]).

SECURITY POLICIES

There are no Organizational Security Policies defined for this evaluation as there are not defined in the [GPOSPP].

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions specified in the [GPOSPP] and included in the [ST], are constraints to the conditions used to assure the security properties and functionalities compiled by the security target [ST]. 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.

Assumption	Description
A.PLATFORM	The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.
A.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope.
A.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

THREATS

The threats to the IT assets against which protection is required by the TOE or by the security environment as defined in the [GPOSPP] and included in the [ST] are listed below.

Threat	Description
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS.
T.LOCAL_ATTACK	An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.
T.LIMITED_PHYSICAL_ACCESS	An attacker may attempt to access data on the OS while having a limited amount of time with the physical device.

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 in the [GPOSPP] and included in the [ST] are categorized below.

Environment Objective	Description
OE.PLATFORM	The OS relies on being installed on trusted hardware.
OE.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use.
OE.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise policy.

ARCHITECTURE

LOGICAL ARCHITECTURE

The operating system (OS) is the core of an information system. It ensures normal operation of upper layer applications, such as network services and database systems. However, application-layer security mechanisms alone cannot solve security problems of information systems fundamentally. Without the system-layer security mechanisms, application-layer security mechanisms are vulnerable to damages, bypasses, and spoofing attacks. Application-layer security mechanisms, such as access control and encryption, rely on system-layer security mechanisms. EulerOS provides security mechanisms, such as identity authentication, security protocols, fine-grained access control, mandatory access control, file integrity check, security audit, memory object reuse, and trusted path.

These security mechanisms lay the security basis for upper layer applications.

The security architecture is described as follows:

● Security hardening tools: enable the easy-to-use security configuration and management by providing security hardening for system services, file permissions, kernel parameters, log audit, and accounts and passwords of EulerOS.

● IDENT: implements user identification and authentication.

● SAK: provides security attention keys for trusted path to start the trusted login process.

● ACL: implements fine-grained discretionary access control based on the access control list.

● LSM: Linux security module.

● CAP: implements mandatory access control (MAC) based on the LSM.

● AUDIT: implements security audit.

● MOR: prohibits memory object reuse.

● SP: security protocols integrated by EulerOS.

PHYSICAL ARCHITECTURE

The following physical and virtual hardware platforms, corresponding firmware, and components are supported by the TOE:

● FusionCube 6000 and 6000C (with TPM chip embedded)
● FusionServer RH2288H V3 Rack Server (with TPM chip embedded)
● FusionServer RH8100 V3 Rack Server (with TPM chip embedded)
● FusionServer X6800 Data Center Server (with TPM chip embedded)
● FusionServer XH628 V3 Server Node (with TPM chip embedded)
● Linux QEMU-KVM-1.5.3 virtual platform (with virtualized TPM chip)

The TOE was evaluated on the following physical platform:

● FusionServer RH2288H V3 Rack Server (with TPM chip embedded).

Note: The TPM chip used in evaluation is Infineon SLB9665.

DOCUMENTS

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

● Huawei EulerOS V2.0 Installation Guide, Version 0.2

● Huawei EulerOS V2.0 User Guide, Version 0.2

PRODUCT TESTING

The tests performed by the evaluator are based on the assurance activities defined for the ATE activity in the [GPOSPP] for each SFR that is included in the [ST].

The evaluator has performed an installation and configuration of the TOEs and their operational environment following the steps included in the installation and operation manual. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to security target [ST].

The independent testing has covered 100% of SFRs of the [ST] and assurance activities defined in the [GPOSPP] for each SFR. There has not been any deviation from the expected results under the environment defined in security target [ST].

PENETRATION TESTING

According to the [GPOSPP], the vulnerability analysis scope has taken into account the public vulnerabilities affecting to all components of the operating system. The lab has performed a search on public sources to discover known vulnerabilities of the TOE.

The evaluator has ensured that for all the public vulnerabilities identified in the TOE belonging to the period from January 26, 2017 to December 20, 2017, the vendor has applied a patch over the affected components to fix the vulnerabilities or has provided a rationale in order to demonstrate its non-applicability.

EVALUATED CONFIGURATION

The TOE was evaluated on the following physical platform:

● FusionServer RH2288H V3 Rack Server (with TPM chip embedded).

Note: The TPM chip used in evaluation is Infineon SLB9665.

EVALUATION RESULTS

The product EulerOS v2.0 build 3.10.0-327.59.59.46.h34.x86_64 has been evaluated against the EulerOS 2.0 Security Target, version 0.9, 2017-12-20.

All the assurance components defined in the [GPOSPP] 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 assurances packages defined in the [GPOSPP] and included in the [ST], as defined by the Common Criteria v3.1 R5, the [GPOSPP] 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.

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. The following usage recommendations are given:

- 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

Considering the obtained evidences during the instruction of the certification request of the product EulerOS v2.0 build 3.10.0-327.59.59.46.h34.x86_64, 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.

[GPOSPP] NIAP - Protection Profile for General Purpose Operating Systems, Version: 4.1, 2016-03-09

[ST] EulerOS 2.0 Security Target, version 0.9, 2017-12-20.

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:

- EulerOS 2.0 Security Target, version 0.9, 2017-12-20.

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 selected.