Reference: 2020-38-INF-3828- v2
Target: Pública
Date: 15.07.2022

Created by: I003
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2020-38**
TOE	**Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software version V200R019C10SPC800 Patch V200R019SPH008T**
Applicant	**B84136464 - Huawei Technologies España, S.L.**
References	

[EXT-6174] Certification Request

[EXT-7752] Evaluation Technical Report

Certification report of the product Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software version V200R019C10SPC800 Patch V200R019SPH008T, as requested in [EXT-6174] dated 20/07/2020, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-7752] received on 10/05/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software version V200R019C10SPC800 Patch V200R019SPH008T.

The TOE is a switches product series (network devices) that provide stable, reliable, and high-performance layer 2 and layer 3 switching services.

Developer/manufacturer: Huawei Technologies España, S.L.

Sponsor: Huawei Technologies España, S.L..

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

ITSEF: DEKRA Testing and Certification S.A.U.

Protection Profile: collaborative Protection Profile for Network Devices (v2.1), 24 September 2018.

Evaluation Level: Common Criteria v3.1 R5 (assurance packages according to the [cPP_ND_21]).

Evaluation end date: 26/05/2022

Expiration Date[1]: 16/07/2027

All the assurance components required by the evaluation level of the [cPP_ND_21] have been assigned a “PASS” verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the [cPP_ND_21] assurance level packages, as defined by the Common Criteria v3.1 R5, the [cPP_ND_21] and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software version V200R019C10SPC800 Patch V200R019SPH008T, a positive resolution is proposed.

TOE SUMMARY

The TOE is HUAWEI CE16800&CE12800&CE8800&CE6800 Series Switches, which consists of the following products: CE16804, CE16808, CE16816, CE12804, CE12808, CE12816, CE8861-4C-EI, CE8850-64CQ-EI, CE6863-48S6CQ, CE6881-48S6CQ and CE6820-48S6CQ. The software running on

[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.

these devices is the Versatile Routing Platform (VRP) software version V200R019C10SPC800 patch V200R019SPH008T, that is a network OS incorporating Huawei's proprietary intellectual properties and capable of supporting various network systems of Huawei.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the assurance packages defined in the [cPP_ND_21] according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_FSP.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.1
	ALC_CMS.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.1
	ASE_REQ.1
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_IND.1
AVA	AVA_VAN.1

SECURITY FUNCTIONAL REQUIREMENTS

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

SECURITY FUNCTIONAL REQUIREMENT
FAU_GEN.1
FAU_GEN.2
FAU_STG_EXT.1
FCS_CKM.1
FCS_CKM.2
FCS_CKM.4
FCS_COP.1/DataEncryption

FCS_COP.1/SigGen
FCS_COP.1/Hash
FCS_COP.1/KeyedHash
FCS_RBG_EXT.1
FIA_AFL.1
FIA_PMG_EXT.1
FIA_UIA_EXT.1
FIA_UAU_EXT.2
FIA_UAU.7
FMT_MOF.1/ManualUpdate
FMT_MTD.1/CoreData
FMT_SMF.1
FMT_SMR.2
FPT_SKP_EXT.1
FPT_APW_EXT.1
FPT_TST_EXT.1
FPT_TUD_EXT.1
FPT_STM_EXT.1
FTA_SSL.3
FTA_SSL.4
FTA_SSL_EXT.1
FTA_TAB.1
FTP_ITC.1
FTP_TRP.1/Admin
FAU_STG.1
FAU_STG.3/LocSpace
FCS_SSHS_EXT.1
FCS_TLSC_EXT.2
FIA_X509_EXT.1/Rev
FIA_X509_EXT.2
FMT_MOF.1/Services
FMT_MTD.1/CryptoKeys

IDENTIFICATION

Product: Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software version V200R019C10SPC800 Patch V200R019SPH008T

Security Target: Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software V200R019C10SPC800 Security Target, v1.10 (10 May 2022).

Protection Profile: collaborative Protection Profile for Network Devices, v2.1 (24 September 2018).

Evaluation Level: Common Criteria v3.1 R5 (assurance packages according to the [cPP_ND_21]).

SECURITY POLICIES

The use of the product Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software version V200R019C10SPC800 Patch V200R019SPH008T 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 3.4 ("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 CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software version V200R019C10SPC800 Patch V200R019SPH008T, although the agents implementing attacks have the attack potential according to the Basic of the [cPP_ND_21] 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 3.2 ("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 4.1 ("Security Objectives for the operational Environment").

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Security audit

  The log module of the host software records operations on a device and events that occur to a device. The recorded operations and events are log messages. Log messages provide evidence for diagnosing and maintaining a system. Log messages reflect the operating status of a device and are used to analyze the conditions of a network and to find out the causes of network failure or faults.

- Cryptography support

  The TOE provides cryptography in support of secure connections that includes remote administrative management.

- Identification and authentication

  The authentication functionality provides validation by user's account name and password. Public key authentication is supported for SSH users. Detailed functionalities, for example max idle-timeout period, max log-in attempts, UI lock, user kick out, can be applies by administrator according to networking environment, customized security considerations, differential user role on TOE, and/or other operational concerns.

- Secure Management

  The TOE restricts the ability to determine the behavior of and modify the behavior of the functions transmission of audit data to the security administrator. Only the security administrator can manage the cryptographic keys. Protection of the TSF

  The TOE protects the pre-shared keys, symmetric keys, and private keys from reading them by an unauthorized entity. The TOE stores the users or administrator passwords in non-plaintext form preventing them from reading. The TOE verifies the packet before their installation and uses the digital signature.

- TOE access through user authentication

  The TOE provides communication security by implementing SSH protocol.

- Trusted path and channels for device authentication

  The TOE supports the trusted connections using TLS for the communication with the audit server.

PHYSICAL ARCHITECTURE

The physical scope of the TOE is described below:

Hardware:

Model	Hardware
CE16804	CE16804 Integrated Chassis, 2 slots for MPU（Main Processing Unit), 9 slots for SFU, 4 slots for LPU (Line Processing Unit)
CE16808	CE16808 Integrated Chassis, 2 slots for MPU（Main Processing Unit), 9 slots for SFU, 8 slots for LPU (Line Processing Unit)
CE16816	CE16816 Integrated Chassis, 2 slots for MPU（Main Processing Unit), 9 slots for SFU, 16 slots for LPU (Line Processing Unit)
CE12804	CE12804 Integrated Chassis, 2 slots for MPU（Main Processing Unit), 6 slots for SFU, 4 slots for LPU (Line Processing Unit)
CE12808	CE12808 Integrated Chassis, 2 slots for MPU（Main Processing Unit), 6 slots for SFU, 8 slots for LPU (Line Processing Unit)
CE12816	CE12816 Integrated Chassis, 2 slots for MPU（Main Processing Unit), 6 slots for SFU, 16 slots for LPU (Line Processing Unit)
CE8861-4C-EI	With 4 Subcard Slots, Without FAN Box and Power Module
CE8850-64CQ-EI	64-Port 10GE QSFP28, 2-Port 10GE QSFP+, Without Fan and Power Module
CE6881-48S6CQ	48-port 10G interface and 6-port 100G interface TOR
CE6820-48S6CQ	48-port 10G interface and 6-port 100G interface TOR

Software package:

Platform	Package name	Item version	Signature file
CE16800 series	CE16800-V200R019C10SPC800.cc	V200R019C10SPC800	CE16800-V200R019C10SPC800.cc.asc
CE12800 series	CE12800-V200R019C10SPC800.cc	V200R019C10SPC800	CE12800-V200R019C10SPC800.cc.asc
CE8800 series	CE8850EI-V200R019C10SPC800.cc	V200R019C10SPC800	CE8850EI-V200R019C10SPC800.cc.asc
	CE8861EI-V200R019C10SPC800.cc	V200R019C10SPC800	CE8861EI-V200R019C10SPC800.cc.asc
CE6800 series	CE6881EI-V200R019C10SPC800.cc	V200R019C10SPC800	CE6881EI-V200R019C10SPC800.cc.asc
	CE6820-V200R019C10SPC800.cc	V200R019C10SPC800	CE6820-V200R019C10SPC800.cc.asc

	CE6863-V200R019C10SPC800.cc	V200R019C10SPC800	CE6863-V200R019C10SPC800.cc.asc

Patch:

Platform	Patch name	Item version	Signature file
CE16800 series	CE16800-V200R019SPH008T.pat	V200R019SPH008T	CE16800-V200R019SPH008T.pat.asc
CE12800 series	CE12800-V200R019SPH008T.pat	V200R019SPH008T	CE12800-V200R019SPH008T.pat.asc
CE8800 series	CE8850EI-V200R019SPH008T.pat	V200R019SPH008T	CE8850EI-V200R019SPH008T.pat.asc
	CE8861EI-V200R019SPH008T.pat	V200R019SPH008T	CE8861EI-V200R019SPH008T.pat.asc
CE6800 series	CE6881EI-V200R019SPH008T.pat	V200R019SPH008T	CE6881EI-V200R019SPH008T.pat.asc
	CE6820-V200R019SPH008T.pat	V200R019SPH008T	CE6820-V200R019SPH008T.pat.asc
	CE6863-V200R019SPH008T.pat	V200R019SPH008T	CE6863-V200R019SPH008T.pat.asc

DOCUMENTS

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

Document name	Version
Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software V200R019C10SPC800 Operational user Guidance.pdf	1.5
Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software V200R019C10SPC800 Preparative Procedures.pdf	1.5
CloudEngine 16800 Series Switches V200R019C10 Product Documentation.chm	0.5
CloudEngine 12800 and 12800E Series Switches V200R019C10 Product Documentation.chm	0.6
CloudEngine 8800, 7800, 6800, and 5800 Series Switches V200R019C10 Product Documentation.chm	0.6

PRODUCT TESTING

Huawei has chosen CloudEngine 16804 as the Reference/ Canonical TOE. Additionally, the developer has produced a rationale (TRR) describing its strategy for reusing test results of the Reference TOE based upon the DAR.

The whole evaluation has been performed on the Reference TOE (CloudEngine 16804). All SFRs have been tested according to the [cPP_ND_21] and [cPP_ND_21_SD]. For the remaining devices include in the product series the testing of the requirements that could be performed in remote has been tested in Huawei Development Center, on the other hand, the requirements that need physical interaction or those that due to their complexity or importance had been chosen under the evaluator's criteria has been tested in the Reference TOE in Dekra T&C Laboratory.

The evaluator has designed a set of tests following a suitable strategy for the TOE type taking into account:

- All SFRs have been tested following the procedures defined in the supporting document [cPP_ND_21_SD].
- Increasing test coverage of the four TSFIs (IF_SYSLOG, IF_SSH, IF_CLI and IF_NTP) varying the input parameters: search for critical parameters in the TSFIs and the incorrect behaviour suspicion with specific input values.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below.

Therefore, for the operation of the product Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software version V200R019C10SPC800 Patch V200R019SPH008T it is necessary the disposition of the following software components:

- Versatile Routing Platform (VRP) software version V200R019C10SPC800 patch V200R019SPH008T

Regarding the hardware components, the TOE includes the following platforms:

- CE16804
- CE16808
- CE16816
- CE12804
- CE12808
- CE12816
- CE8861-4C-EI
- CE8850-64CQ-EI
- CE6863-48S6CQ
- CE6881-48S6CQ
- CE6820-48S6CQ

EVALUATION RESULTS

The product Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software version V200R019C10SPC800 Patch V200R019SPH008T has been evaluated against the Security Target Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software V200R019C10SPC800 Security Target, v1.10 (10 May 2022).

All the assurance components required by the evaluation level of the [cPP_ND_21] have been assigned a "PASS" verdict. Consequently, the laboratory DEKRA Testing and Certification S.A.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the [cPP_ND_21] assurance level packages, as defined by the Common Criteria v3.1 R5, the [cPP_ND_21] 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. Nonetheless, the following usage recommendations are given:

- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.
- The application of all firewall rules according to the preparative procedures are extremely important to maintain the security in the TOE environment denying all external access to the TOE.
- The application of the TLS encryption after the installation procedures is critical to maintain the communication secure and safeguard the TOE assets.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software version V200R019C10SPC800 Patch V200R019SPH008T, 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.

[cPP_ND_21] collaborative Protection Profile for Network Devices, v2.1 (24 September 2018).

[cPP_ND_21_SD] Evaluation activities for Network Devices cPP, v2.1 (September 2018).

[ST] Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software V200R019C10SPC800 Security Target, v1.10 (10 May 2022).

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:

- Huawei CE16800&CE12800&CE8800&CE6800 Series Switches running VRP software V200R019C10SPC800 Security Target, v1.10 (10 May 2022).

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 selected.