Reference: 2020-42-INF-3839- v1
Target: Pública
Date: 26.07.2022

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

CERTIFICATION REPORT

Dossier #	**2020-42**
TOE	**Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300**
Applicant	**B84136464 - Huawei Technologies España, S.L.**
References	

[EXT-6184] Solicitud de certificacion. Huawei NE40E&NetEngine 8000 Series Routers

[EXT-7717] to [EXT-7724] Evaluation Technical Report

Certification report of the product Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300, as requested in [EXT-6184] dated 01/06/2020, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-7717] a [EXT-7724] received on 25/03/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300.

The TOE is a network device that is connected to the network and has an infrastructure role within the network.

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: Applus Laboratories.

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: 27/05/2022

Expiration Date[1]: 15/07/2027

All the assurance components required by the evaluation level of the [cPP_ND_21] have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories 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 NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300, a positive resolution is proposed.

TOE SUMMARY

The TOE is NE40E&NetEngine 8000 series routers which consists of the following products: NE40E-M2K, NE40E-M2K-B, NE40EX2- M14, NE40E-X8A, NE40E-X16A, NetEngine 8000 F1A-8H20Q, NetEngine 8000 M1A, NetEngine 8000 M6, NetEngine 8000 M8, NetEngine 8000 M14, NetEngine 8000 X4 and NetEngine 8000 X8. The software running on these devices is the Versatile Routing

[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.

Platform (VRP) software version V800R012C00SPC300, 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_TAB.1
FTP_ITC.1
FTP_TRP.1/Admin
FAU_STG.1
FAU_STG.3/LocSpace
FCS_SSHC_EXT.1
FCS_SSHS_EXT.1
FCS_TLSC_EXT.1
FIA_X509_EXT.1/Rev
FIA_X509_EXT.2
FMT_MOF.1/Services
FMT_MTD.1/Functions
FMT_MTD.1/CryptoKeys

IDENTIFICATION

Product: Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300

Security Target: [ST] Security target of Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300 v1.33. Date: 2022-02-09

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 NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300 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 3.3 ("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 3.2 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300, 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 3.1 ("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 4.1 ("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
NE40E-M2K	NE40E-M2K Integrated Chassis, 1 slot for fixed interfaces, 2 slots for PIC (Physical Interface Card)
NE40E-M2K-B	NE40E-M2K-B Integrated Chassis, 1 slots for fixed interfaces, 2 slots for PICs (Physical Interface Card)
NE40E-X2-M14	NE40E-X2-M14 Integrated Chassis, 2 slots for IPU (Integrated Network Processing Unit), 14 slots (DC) or 10 slots (AC) for PIC
NE40E-X8A	NE40E-X8A Integrated Chassis, 2 slots for SRU (Switch and Route Processing Unit), 2 slots for SFU (Switch Fabric Unit), 8 slots for LPU
NE40E-X16A	NE40E-X16A Integrated Chassis, 2 slots for MPU（Main Processing Unit), 4 slots for SFU,16 slots for LPU (Line Processing Unit)
NetEngine 8000 F1A-8H20Q	NetEngine 8000 F1A-8H20Q Integrated Chassis,Fixed interfaces
NetEngine 8000 M1A	NetEngine 8000 M1A Integrated Chassis,Fixed interfaces
NetEngine 8000 M6	NetEngine 8000 M6 Integrated Chassis, 2 slots for CXP (System Control, Cross-connect and Multiprotocol Process Unit), 6 slots (DC) or 4 slots (AC) for PIC
NetEngine 8000 M8	NetEngine 8000 M8 Integrated Chassis, 2 slots for IPU, 8 slots (DC) or 6 slots (AC) for PIC
NetEngine 8000 M14	NetEngine 8000 M14 Integrated Chassis, 2 slots for IPU, 14 slots (DC) or 10 slots (AC) for PIC
NetEngine 8000 X4	NetEngine 8000 X4 Integrated Chassis, 2 slots for MPU, 8 slots for SFU, 4 slots for LPU
NetEngine 8000 X8	NetEngine 8000 X8 Integrated Chassis, 2 slots for MPU, 8 slots for SFU, 8 slots for LPU

Software

Model	Software
NE40E-M2K	NE40E-M2K-V800R012C00SPC300.cc
NE40E-M2K-B	NE40E-M2K-B-V800R012C00SPC300.cc
NE40E-X2-M14	NE40E-X2-M14-V800R012C00SPC300.cc
NE40E-X8A	NE40E-X8A-X16A-V800R012C00SPC300.cc
NE40E-X16A	NE40E-X8A-X16A-V800R012C00SPC300.cc

NetEngine 8000 F1A- 8H20Q	NetEngine8000-F1A-8H20Q-V800R012C00SPC300.cc
NetEngine 8000 M1A	NetEngine8000-M1A-V800R012C00SPC300.cc
NetEngine 8000 M6	NetEngine8000-M6-V800R012C00SPC300.cc
NetEngine 8000 M8	NetEngine8000-M8-V800R012C00SPC300.cc
NetEngine 8000 M14	NetEngine8000-M14-V800R012C00SPC300.cc
NetEngine 8000 X4	NetEngine8000-X-V800R012C00SPC300.cc
NetEngine 8000 X8	NetEngine8000-X-V800R012C00SPC300.cc

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
AGD_OPE Huawei NE40E&NetEngine 8000 Series Routers V800R012 Operational user Guidance.pdf	1.16
AGD_PRE Huawei NE40E&NetEngine 8000 Series Routers V800R012 Preparative Procedures.pdf	1.17
AGD_C&R Huawei NE40E&NetEngine 8000 Series Products V800R012 Configuration and Reference.pdf	1.16
NE40E V800R012C00SPC300 Product Documentation	04
NE40E-M2H and M2K V800R012C00SPC300 Product Documentation	04
NE40E-X2-M14 Router V800R012C00 Product Documentation	04
NetEngine 8000 X V800R012C00SPC300 Product Documentation	04
NetEngine 8000 F V800R012C00SPC300 Product Documentation	04
NetEngine 8000 M1A and M6 V800R012C00SPC300 Product Documentation	05
NetEngine 8000 M14 and M8 V800R012C00SPC300 Product Documentation	04

PRODUCT TESTING

NetEngine 8000 M14 was reference 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 (NetEngine 8000 M14). All SFRs have been tested according to the [cPP_ND_21] and [cPP_ND_21_SD]. Additonally, the laboratory performed testing activities on other two models: NE40E-MK2-B on its premises and NetEngine 8000 M8 remotely.

EVALUATED CONFIGURATION

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

Therefore, for the operation of the product Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300 it is necessary the disposition of the following software components:

- Versatile Routing Platform (VRP) software version V800R012C00SPC300

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

- NE40E-M2K
- NE40E-M2K-B
- NE40E-X2-M14
- NE40E-X8A
- NE40E-X16A
- NetEngine 8000 F1A- 8H20Q
- NetEngine 8000 M1A
- NetEngine 8000 M6
- NetEngine 8000 M8
- NetEngine 8000 M14
- NetEngine 8000 X4
- NetEngine 8000 X8

EVALUATION RESULTS

The product Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300 has been evaluated against the Security Target [ST] Security target of Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300 v1.33. Date: 2022-02-09.

All the assurance components required by the evaluation level of the [cPP_ND_21] 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 [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 evaluation team makes the following security recommendations:

- 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 NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300, 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] Security target of Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300 v1.33. Date: 2022-02-09

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:

- [ST] Security target of Huawei NE40E&NetEngine 8000 Series Routers running VRP software V800R012C00SPC300 v1.33. Date: 2022-02-09

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.