Reference: 2020-49-INF-4353- v1
Target: Limitada al expediente
Date: 14.08.2024

Created by: CERT11
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2020-49**
TOE	**Huawei CX600 and PTN 6900 Series Routers running VRP software version V800R021C00SPC100**
Applicant	**B84136464 - Huawei Technologies España, S.L.**

References

[EXT-6288] Certification Request

[EXT-8975] to [EXT-8980] Evaluation Technical Report

Certification report of the product Huawei CX600 and PTN 6900 Series Routers running VRP software version V800R021C00SPC100, as requested in [EXT-6288] dated 31/08/2020, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-8975] to [EXT-8980] received on 08/03/2024.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei CX600 and PTN 6900 Series Routers running VRP software version V800R021C00SPC100.

The TOE is CX600&PTN 6900 Series Routers running VRP software comprised of both software and hardware. The software is comprised of Versatile Routing Platform (VRP) software, VRP is a network OS incorporating Huawei's proprietary intellectual properties and capable of supporting various network systems of Huawei. The hardware is comprised of the following: CX600-M2K, CX600-M2K-B, CX600-X8A, CX600-X16A, PTN 6900-M2K, PTN 6900-M2K-B, PTN 6900-2-M8C, PTN 6900-2-M14.

The Huawei CX600&PTN 6900 Series Routers running VRP software use the same VRP version. TSF relevant functions depend on software implementation.

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

Sponsor: Huawei Technologies España, S.L..

Certification Body: Centro Criptológico Nacional (CCN).

ITSEF: Applus Laboratories.

Protection Profile: Collaborative Protection Profile for Network Devices, Version 2.1, 24-Sep-2018 (archived on 11/01/2022).

Evaluation Level: Common Criteria 3.1 R5 (assurance packages according to the [CPP_ND]).

Evaluation end date: 13/06/2024

Expiration Date[1]: 31/07/2029

All the assurance components required by the evaluation level of the [CPP_ND] 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], as defined by the Common Criteria 3.1 R5 and the CEM 3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product Huawei CX600 and PTN 6900 Series Routers running VRP software version V800R021C00SPC100, a positive resolution is proposed.

[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.

TOE SUMMARY

The TOE is CX600&PTN 6900 Series Routers running VRP software comprised of both software and hardware. The software is comprised of Versatile Routing Platform (VRP) software, VRP is a network OS incorporating Huawei's proprietary intellectual properties and capable of supporting various network systems of Huawei. The hardware is comprised of the following: CX600-M2K, CX600-M2K-B, CX600-X8A, CX600-X16A, PTN 6900-M2K, PTN 6900-M2K-B, PTN 6900-2-M8C, PTN 6900-2-M14.

The Huawei CX600&PTN 6900 Series Routers running VRP software use the same VRP version. TSF relevant functions depend on software implementation.

The physical scope comprises the following hardware appliances and the TOE software:

- Appliances: CX600-M2K, CX600-M2K-B, CX600-X8A, CX600-X16A, PTN 6900-M2K, PTN 6900-M2K-B, PTN 6900-2-M8C, PTN 6900-2-M14
- Software: CX600&PTN 6900 Router V800R021C00SPC100, CX600-M2K-B, CX600-X8A, CX600-X16A, PTN 6900-M2K, PTN 6900-M2K-B, PTN 6900-2-M8C, PTN 6900-2-M14

There are only hardware differences between different devices. All the routers share the same platform so the SFRs are the same. Network management server, local console and syslog server are supported by all TOE evaluated configurations. The TOE only has one configuration.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level of the [CPP_ND] to the table, according to Common Criteria 3.1 release 5.

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_FSP.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.1
	ALC_CMS.1
ATE	ATE_IND.1

AVA	AVA_VAN.1

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to Common Criteria version 3.1 release 5 assurance packages according to the Collaborative Protection Profile for Network Devices, Version 2.1, 24-Sep-2018.

The detail of these security functional requirements is documented in the Security Target [ST], section 6 ("Security Functional Requirements").

IDENTIFICATION

Product: Huawei CX600 and PTN 6900 Series Routers running VRP software version V800R021C00SPC100

Security Target: Huawei CX600&PTN 6900 Series Routers running VRP software Security Target, version 1.15, 17/11/2023.

Protection Profile: Collaborative Protection Profile for Network Devices, Version 2.1, 24-Sep-2018. (archived on 11/01/2022).

Evaluation Level: Common Criteria 3.1 R5 (assurance packages according to the [CPP_ND]).

SECURITY POLICIES

The use of the product Huawei CX600 and PTN 6900 Series Routers running VRP software version V800R021C00SPC100 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 CX600 and PTN 6900 Series Routers running VRP software version V800R021C00SPC100, although the agents implementing attacks have the attack potential according to the to the attack potential of the [CPP_ND] 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.

(1) 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.

Key elements of log messages include timestamp, host name, Huawei identifier, version number, module name, log level, description of log, information type, system component ID and information about details.

IC component are the module processing, outputting log records. Information hierarchy is designed to help the user roughly differentiate between information about normal operation and information about faults. Since the information center needs to output information to the terminal, console, log buffer, and log file.

(2) Cryptographic support

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

The cryptographic services provided by the TOE are described in Table below.

Cryptography provided by TOE

Cryptography Function	Use in the TOE
DRBG	Used in session establishment of TLS and SSH
ECDH	Used in session establishment of SSH
DHE	Used in session establishment of TLS
SHA	Used to provide cryptographic hashing services
HMAC-SHA	Used to provide integrity and authentication verification
AES	Used to encrypt traffic transmitted through TLS and SSH
RSA	Used in the authentication of TLS
ECDSA	Used in the authentication of SSH

(3) 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, account 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.

(4) 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. Only the security administrator has the right of opening/closing the security services and creation/deletion/modification of the user accounts.

(5) 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.

(6) TOE access through user authentication

The TOE provides communication security for remote administrative session by implementing SSH protocol.

To protect the TOE from eavesdrop and to ensure data transmission security and confidentiality, SSH implements:

- authentication by password or by public-key;
- AES encryption algorithms;
- secure cryptographic key exchange;
- Besides default TCP port 22, manually specifying a listening port is also implemented since it can effectively reduce attack.

The TOE supports password-based authentication for local administrative session.

(7) Trusted path and channels for device authentication

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

The TOE protects communications between a TOE and authorized remote administrator with SSH.

PHYSICAL ARCHITECTURE

This section will define the physical scope of the Huawei CX600&PTN 6900 Series Routers running VRP Software to be evaluated.

Type	Delivery Item	Version
Hardware	CX600-M2K, CX600-M2K-B, CX600-X8A, CX600-X16A, PTN 6900-M2K, PTN 6900-M2K-B, PTN 6900-2-M8C, PTN 6900-2-M14 The Hardware will be delivered by air, ship, train or automobile.	NA
Software	CX600&PTN 6900 Router V800R021C00SPC100 Format: CX600-M2K : CX600-M2K_V800R021C00SPC100.cc Digital signature: CX600-M2K_V800R021C00SPC100.cc.asc Info:	V800R021C00SPC100

Type	Delivery Item	Version
	User can obtain the software package directly from the local support engineer. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website) HASH SHA256: 07020586a60abbc30e42091b327ce67164610eb164737be9f94687c62507b632 CX600-M2K-B：CX600-M2K-B_V800R021C00SPC100.cc Digital signature: CX600-M2K-B_V800R021C00SPC100.cc.asc Info: User can obtain the software package directly from the local support engineer. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website) HASH SHA256: f5a2d9324a9b3fbfac0a94fc7d6dbd36c1258255cedd00016def48c213e2b608 CX600-X8A: CX600-X8A-X16A_V800R021C00SPC100.cc Digital signature: CX600-X8A-X16A_V800R021C00SPC100.cc.asc Info: User can obtain the software package directly from the local support engineer. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website) HASH SHA256: d169db6a2db1e34703004a60d61c45bd3a728c53b26f23e9eca4e5423125dd18	

Type	Delivery Item	Version
	CX600-X16A: CX600-X8A-X16A_V800R021C00SPC100.cc Digital signature: CX600-X8A-X16A_V800R021C00SPC100.cc.asc Info: User can obtain the software package directly from the local support engineer. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website) HASH SHA256: d169db6a2db1e34703004a60d61c45bd3a728c53b26f23e9eca4e5423125dd18 PTN 6900-M2K : PTN6900-M2K_V800R021C00SPC100.cc Digital signature: PTN6900-M2K_V800R021C00SPC100.cc.asc Info: User can obtain the software package directly from the local support engineer. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website) HASH SHA256: 9be57cf3fce417510017b8e5840715db18b4161ff26c33d45e7a58d1d28f5265 PTN 6900-M2K-B: PTN6900-M2K-B_V800R021C00SPC100.cc Digital signature: PTN6900-M2K-B_V800R021C00SPC100.cc.asc Info: User can obtain the software package directly from the local support engineer. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website)	

Type	Delivery Item	Version
	HASH SHA256: 9a11f20017efb222e9313e9d284a88fa5d25deb6005beac9b1d8c4a6a36ecd62 PTN 6900-2-M8C：PTN6900-2-M8C-M14_V800R021C00SPC100.cc Digital signature: PTN6900-2-M8C-M14_V800R021C00SPC100.cc.asc Info: User can obtain the software package directly from the local support engineer. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website) HASH SHA256: 132163028f96f6935bd4422646cf6566dd72dcba7d4a55096dc9ad91d8bcc40c PTN 6900-2-M14 : PTN6900-2-M8C-M14_V800R021C00SPC100.cc Digital signature: PTN6900-2-M8C-M14_V800R021C00SPC100.cc.asc Info: User can obtain the software package directly from the local support engineer. Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website) HASH SHA256: 132163028f96f6935bd4422646cf6566dd72dcba7d4a55096dc9ad91d8bcc40c	
Product guidance	Huawei CX600&PTN 6900 Series Routers V800R021C00SPC100 Operational user Guidance	1.7

Type	Delivery Item	Version
	Info: The documentation is delivered by email in PDF format. HASH SHA256: 97d7443518cfc30dc1014ed7c34cf7a7a1a005986115972820c7d0b214db867a	
	Huawei CX600&PTN 6900 Series Routers V800R021C00SPC100 Preparative Procedures Info: The documentation is delivered by email in PDF format. HASH SHA256: b2d7dbe305221415644bd6f2f87d70ac61059ceb847c9cab0c0c4772679bf943	1.7
	Huawei CX600&PTN 6900 Series Routers V800R021C00SPC100 Configuration and Reference Info: The documentation is delivered by email in PDF format. HASH SHA256: 9fa895c1b4ef8865bd33cd071847916b707346225a863229557c7588d5cfd0b0	1.4
	HUAWEI CX600 Product Documentation Product Version: V800R021C00 Library Version: 03 Date: 2021-12-31 HASH SHA256: B210EC09B884AD2DE0EE3142E02F62A63D4E9DB14DFAF54ECF6C1AA03B290211 HUAWEI CX600-M2 Product Documentation Product Version: V800R021C00 Library Version: 03 Date: 2021-12-31 HASH SHA256:	refers to the "Library Version" shown in the left column

Type	Delivery Item	Version
	0A08951F5BFFD3DB8EDC1778D32377924DEB02893210299348EE6E8236EF5BDC HUAWEI PTN 6900-M2 Product Documentation Product Version: V800R021C00 Library Version: 03 Date: 2021-12-31 HASH SHA256: FD35813409F4AB82BB2C5914F95CAA6E1F13E5CD81C5B35DDB3BCAB357E107AF HUAWEI PTN 6900-2-M8C, PTN 6900-2-M14 Product Documentation Product Version: V800R021C00 Library Version: 03 Date: 2021-12-31 HASH SHA256: FEDBA960DCA605577918A22EE46B3B04F4699029CF2877B00472942D08F4E2C3 Info: The product documentations are delivered by email. The file format is *.hdx, user can download the *.hdx reader from Huawei support website. These product documentations apply for specific products of child versions belonging to the master product version V800R021C00. The evaluated TOE version V800R021C00SPC100 is considered as one of the child versions belonging to this master product version.	

There are only hardware differences between different devices. All the routers share the same platform so the SFRs are the same. Network management server, local console and syslog server are supported by all TOE evaluated configurations. The TOE only has one configuration.

DOCUMENTS

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

- Huawei CX600&PTN 6900 Series Routers V800R021C00SPC100 Operational user Guidance, version 1.7.
- Huawei CX600&PTN 6900 Series Routers V800R021C00SPC100 Preparative Procedures, version 1.7.
- Huawei CX600&PTN 6900 Series Routers V800R021C00SPC100 Configuration and Reference, version 1.4.
- HUAWEI CX600 Product Documentation, version 03.
- HUAWEI CX600-M2 Product Documentation, version 03.
- HUAWEI PTN 6900-M2 Product Documentation, version 03.
- HUAWEI PTN 6900-2-M8C, PTN 6900-2-M14 Product Documentation, version 03.

PRODUCT TESTING

The evaluator performed the installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to the Security Target [ST].

The product series testing has followed the SOGIS supporting document Evaluation methodology for product series, version 1.0. The ITSEF analysed the Differential Analysis Report (DAR) and Testing Reuse Rationale (TRR) provided by the applicant to prepare the independent testing strategy.

The evaluator has executed the set of tests defined in the Supporting Document of the [CPP_ND] as part of the independent test plan, as required by the protection profile to which the [ST] claims conformance. There has not been any deviation from the expected results under the environment defined in the Security Target [ST].

EVALUATED CONFIGURATION

The acceptance and installation procedures are given in sections 2, 3, 5 and 7 (Secure Acceptance by Production, Secure Installation of the TOE Software by Production, Secure Acceptance by User and Secure Installation of the TOE) of the preparative user guidance Huawei CX600&PTN 6900 Series Routers V800R021C00SPC100 Preparative Procedures v1.7.

EVALUATION RESULTS

The product Huawei CX600 and PTN 6900 Series Routers running VRP software version V800R021C00SPC100 has been evaluated against the Security Target Huawei CX600&PTN 6900 Series Routers running VRP software Security Target, version 1.15, 17/11/2023.

All the assurance components required by the evaluation level of the [CPP_ND] 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], as defined by the Common Criteria 3.1 R5 and the CEM 3.1 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 CX600 and PTN 6900 Series Routers running VRP software version V800R021C00SPC100, a positive resolution is proposed.

In addition to evaluator comments, the certifier recommends TOE consumers to analyse the [ST] to verify that security problem definition and security objectives meets potential consumer needs. Additionally the certifies wants to remark that the used PP for evaluation ([CPP_ND]) meet their sunset date on 11/01/2022.

GLOSSARY

CCN	Centro Criptológico Nacional
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.

[ST] Security target of Huawei CX600&PTN 6900 Series Routers running VRP software, 1.15

[CPP_ND] Collaborative Protection Profile for Network Devices, Version 2.1, 24-Sep-2018. (archived on 11/01/2022).

SECURITY TARGET

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

- Huawei CX600&PTN 6900 Series Routers running VRP software Security Target, version 1.15, 17/11/2023.

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.