Reference: 2019-51-INF-4002- v1
Target: Limitada al expediente
Date: 23.02.2023

Created by: I006
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2019-51**
TOE	**Huawei iSitePower V100R022C00SPC120**
Applicant	**440301192203821 - Huawei Technologies Co., Ltd.**
References	

[EXT-5509] Certification Request

[EXT-8186] Evaluation Technical Report

Certification report of the product Huawei iSitePower V100R022C00SPC120, as requested in [EXT-5509] dated 10/10/2019, and evaluated by DEKRA Testing and Certification S.A.U., as detailed in the Evaluation Technical Report [EXT-8186] received on 21/12/2022.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Huawei iSitePower V100R022C00SPC120.

The iSitePower is a software product running on the Linux operating system based on the ARM chip of the Cortex-A8 architecture for monitoring and managing Huawei's box-type and cabinet-type power systems. It can be accessed through an user Web UI and a LCD panel.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd..

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

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

Protection Profile: N/A.

Evaluation Level: EAL 3 + ALC_FLR.2.

Evaluation end date: 24/01/2023

Expiration Date[1]: 21/02/2028

All the assurance components required by the evaluation level EAL 3 + ALC_FLR.2 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 EAL 3 + ALC_FLR.2, 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 iSitePower V100R022C00SPC120, a positive resolution is proposed.

TOE SUMMARY

The TOE is a software that monitors and manages Huawei's box-type and cabinet-type power systems. It provides a web interface (WebUI) and a LCD Panel that allow users to operate with the TOE in order to change values and parameters.

The TOE provides the following key security features:

- Authentication

[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.

- Authorization
- Auditing
- Security Management
- TOE Access

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL 3 and the evidences required by the additional component ALC_FLR.2 to the table, according to Common Criteria v3.1 R5.

Assurance class	Assurance components
ASE	ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.2 ASE_REQ.2 ASE_SPD.1 ASE_TSS.1
ADV	ADV_ARC.1 ADV_FSP.3 ADV_TDS.2
AGD	AGD_OPE.1 AGD_PRE.1
ALC	ALC_CMC.3 ALC_CMS.3 ALC_DEL.1 ALC_DVS.1 ALC_LCD.1 ALC_FLR.2
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5. Details of security functional requirements can be found in section 6 of the Security Target [ST]

SECURITY FUNCTIONAL REQUIREMENTS

FAU_GEN_EXT.3
FAU_GEN.2
FAU_SAR.1
FAU_SAR.2
FAU_STG.1
FAU_STG.3
FDP_ACC.1
FDP_ACF.1
FIA_AFL.1
FIA_ATD.1
FIA_UAU.2
FIA_UAU.6
FIA_UID.2
FIA_SOS.1
FMT_MOF.1
FMT_MSA.1
FMT_MSA.3
FMT_SMF.1
FMT_SMR.1
FTA_MCS.1
FTA_SSL.3
FTA_SSL.4
FTA_TSE.1
FTA_TAB.1

IDENTIFICATION

Product: Huawei iSitePower V100R022C00SPC120

Security Target: Huawei iSitePower V100R022C00SPC120 Security Target, version 1.14, 14.09.2022

Protection Profile: N/A.

Evaluation Level: EAL 3 + ALC_FLR.2.

SECURITY POLICIES

The use of the product Huawei iSitePower V100R022C00SPC120 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 Policiy”).

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 3.4 (“Assumptions”).

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Huawei iSitePower V100R022C00SPC120, although the agents implementing attacks have the attack potential according to “Basic” of EAL 3 + ALC_FLR.2 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 4.2 (“Security Objectives for the operational Environment”).

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE boundaries from a security functionality point of view is:

- Authentication: The TOE authenticates users based on usernames and passwords. The TOE provides the local authentication mode. The usernames and passwords are stored on the local device. During login, the local usernames and passwords stored on the local device are used for authentication. When a user logs in to the web interface the first time and after the password of a user expires, the user is prompted to change the default password. In addition, password brute force defense mechanism, and automatic lock is performed.

The passwords must meet the complexity requirements defined in the password policy.

- Authorization: The TOE group-based authorization mechanism is used to manage access based on predefined role groups.

  Only authenticated users can perform TOE command operations supported by the users' rights. Only one user group level can be assigned to a user account. Therefore, the user group level of the user is clear at any time.

- Auditing: Logs record the routine maintenance events of the TOE. The TOE users are able to see depending on their role certain logs in order to find security vulnerabilities and risks.

  Logs record operation events related to account management and system configuration, such as changing a password, adding an account, changing a device IP addresses, and other configuration operations.

  The TOE protect the stored audit records in the audit trail from unauthorized deletion and it roll back the oldest records if the audit trail exceeds a certain number of logs.

- TOE Access: A maximum of three users can log in to the web page concurrently. Also the TOE is able to terminate interactive sessions and present appropriate warnings.

- Security management: The TOE provides the functionality to manage user configuration, updates and logs export depending on the user role. Accounts are managed by group. Each group represents specific rights assigned to accounts in the group. The WebUI of the TOE contains three different groups of roles (administrator, engineer and operator) and the LCD Panel contains two groups (administrator and engineer). For example, the accounts in the administrator group have rights to perform all security management and advanced settings operations. Unauthorized operations are not allowed.

PHYSICAL ARCHITECTURE

The SOFTWARE part of the TOE is the following:

Delivery Item	Version	Signature File	Sha256sum hash
iSitePower_V100R022C00SPC120_02X.zip	V100R022C00SPC120	iSitePower_V100R022C00SPC120_2X.zip.asc	a1f168414ed953deb29a51638c9a65504cbaf438ed09acbaeb5853d178e2b53d

The GUIDANCE part of the TOE is the following:

Name of the evidence	Version	Sha256sum hash

Huawei iSitePower V100R022C00SPC120 AGD_OPE v0.4.pdf	0.4	8c8b1c484d45f14540fe8e701e5e817426fe2ef476eb38d8b8f8b41e1d1e7357
Huawei iSitePower V100R022C00SPC120 AGD_PRE V0.4.pdf	0.4	4a59038ca55b203fbbc8cd6bbd440e063d59e67a6eefaa4a8fa86dd4e053edeb

DOCUMENTS

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

- Huawei iSitePower V100R022C00SPC120 AGD_OPE, version 0.4, 14.09.2022.
- Huawei iSitePower V100R022C00SPC120 AGD_PRE, version 0.4, 14.09.2022.

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 all the developer functional tests in the developer premises. Likewise, he has selected and repeated about 25% of the developer functional tests in the testing platform implemented in the evaluation laboratory, selecting one test for each of the most relevant functional class.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Huawei iSitePower V100R022C00SPC120 it is necessary the disposition of the following hardware and software components:

- Huawei's box-type and cabinet-type power system, is the power supply.
- SMU02C, is the Hardware platform where the TOE runs.
- Operating system Linux 4.19.90
- OpenSSL OpenSSL version 1.1.1k
- Browser Firefox 52, Chrome 58, or Internet Explorer 11 or above.
- RAM Memory 4GB RAM

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is the following:

- ETP48400-C3B1: box-type and cabinet-type power system.
- SMU02C: Incorporated in the ETP48400-C3B1
- OS: Linux stm32mp15x 4.19.90
- OpenSSL: OpenSSL version 1.1.1k

EVALUATION RESULTS

The product Huawei iSitePower V100R022C00SPC120 has been evaluated against the Security Target Huawei iSitePower V100R022C00SPC120 Security Target, version 1.14, 14.09.2022.

All the assurance components required by the evaluation level EAL 3 + ALC_FLR.2 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 evaluation level EAL 3 + ALC_FLR.2, 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.

The TOE usage is recommended given that there are not exploitable vulnerabilities for the TOE under its 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.
- The fulfillment 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.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Huawei iSitePower V100R022C00SPC120, a positive resolution is proposed.

The certifier recommends potential TOE consumers to observe Evaluation Team recommendations, strictly following the TOE guidance referenced in section DOCUMENTS and to analyse the assumptions defined in the security problem definition in section 3 of the [ST].

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
ST	Security Target

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] Huawei iSitePower V100R022C00SPC120 Security Target, version 1.14, 14.09.2022.

SECURITY TARGET

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

- Huawei iSitePower V100R022C00SPC120 Security Target, version 1.14, 14.09.2022

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 up to EAL2 and ALC_FLR.