Certification Report

Huawei WLAN AirEngine Series Product running VRP software V200R022C10SPC100

Sponsor and developer: ***Huawei Technologies Co.,Ltd***
Administration Building, Headquarters of Huawei Technologies Co., Ltd., Bantian, Longgang District, Shenzhen, 518129, P.R.C

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-0565198-CR**
Report version:	**1**
Project number:	**0565198**
Author(s):	**Andy Brown**
Date:	**04 December 2023**
Number of pages:	**12**
Number of appendices:	**0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Huawei WLAN AirEngine Series Product running VRP software V200R022C10SPC100. The developer of the Huawei WLAN AirEngine Series Product running VRP software V200R022C10SPC100 is Huawei Technologies Co.,Ltd located in Shenzhen, People's Republic of China and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a series of networking access controllers and access points including both hardware and software. It is defined as the software and the hardware running on the AirEngine devices running WLAN AirEngine Series VRP software.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 04 December 2023 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Huawei WLAN AirEngine Series Product running VRP software V200R022C10SPC100, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Huawei WLAN AirEngine Series Product running VRP software V200R022C10SPC100 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the *[NDcPP]* assurance requirements for the evaluated security functionality.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Huawei WLAN AirEngine Series Product running VRP software V200R022C10SPC100 from Huawei Technologies Co.,Ltd located in Shenzhen, People's Republic of China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	AirEngine 9700-M1	n/a
	AirEngine6761-21T	n/a
	AirEngine6761-21	n/a
	AirEngine6761-21E	n/a
	AirEngine5761-21	n/a
	AirEngine5761-11	n/a
	AirEngine5761-12	n/a
	AirEngine6761-22T	n/a
	AirEngine5761R-11	n/a
	AirEngine5761R-11E	n/a
	AirEngine5761-12W	n/a
	AirEngine5761-11W	n/a
	AirEngine6760-51EI	n/a
Software	WLAN AirEngine Series VRP software	V200R022C10SPC100

To ensure secure usage a set of guidance documents is provided, together with the Huawei WLAN AirEngine Series Product running VRP software V200R022C10SPC100. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

To counter the security threats listed in the [ST], the TOE provides the following security features:

- 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 identity, version, module name, severity, brief description, etc.
- Cryptographic 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 applied by administrator

- 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.
- 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.
    - 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;
        - In addition to default TCP port 22, the feature of manually specifying a listening port is also implemented since it can effectively reduce attacks.
- Trusted path and channels for device authentication
    - The TOE supports the trusted connections using TLS for the communication with the audit server.

The TOE is a standalone TOE, not a distributed TOE as defined in the *[NDcPP]* chapter 3.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.1 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

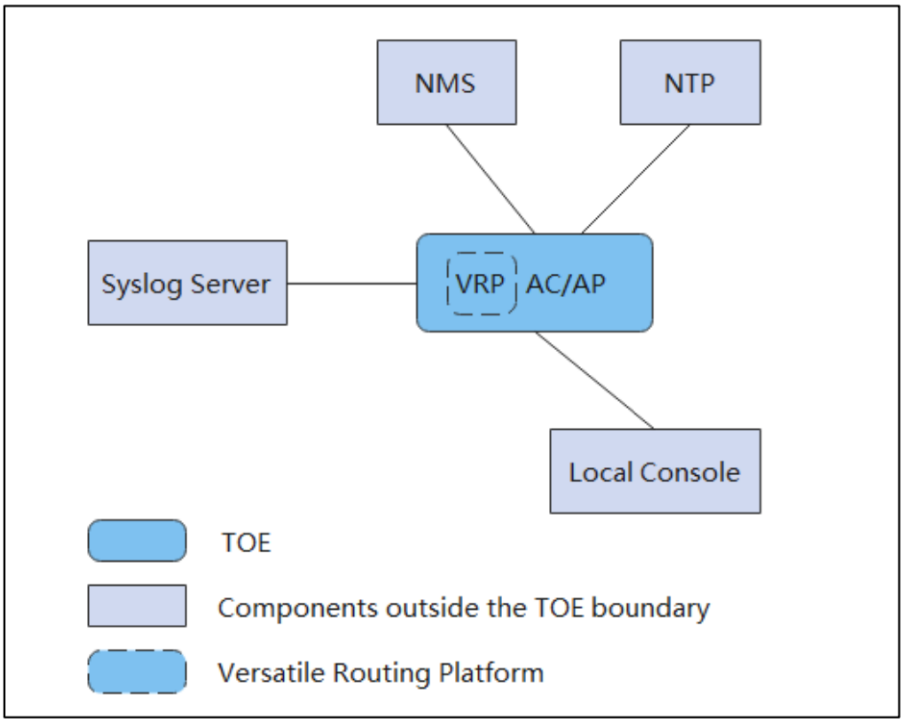
The Huawei WLAN AirEngine series Product running VRP software TOE are used to satisfy the requirements for networks of various scales. .

The TOE includes Access Controllers (AC) and Access Point (AP).

Access Controllers are applicable to Metropolitan Access Networks (MANs) and enterprise networks for wireless access. The AC provides wireless functions through Fit APs. AC Series has a large capacity and high performance. It is security, highly reliable, easy to install and maintain.

The Access Point is the device that provides 802.11-compliant wireless access to connect wired networks to wireless networks.

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Huawei WLAN AirEngine Series Product running VRP software V200R022C10 Operational User Guidance	0.5
Huawei WLAN AirEngine Series Product running VRP software V200R022C10 Preperation Procedure	0.7
WLAN AC, FIT AP, FAT AP, Cloud AP V200R022C10 Upgrade Guide	01
WLAN V200R022C10 Product Documentation	02
Fat AP and Cloud AP V200R022C10 Command Reference	02

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

For the testing performed by the evaluators, the developer provided samples of the TOE and host hardware. The evaluators performed defined tests directly from *[NDcPP]*. During the evaluator analysis phase, no additional independent tests were identified as required to assess the assurance package.

2.6.2 Independent penetration testing

The vulnerability assessment was performed following the guideline provided in *[NDcPP]* Appendix A, based on the following hypotheses:

- Type 1: Public – Vulnerability based
- Type 2: iTC Sourced
- Type 3: Evaluation-Team Generated
- Type 4: Tool Generated

Penetration tests were created based on the vulnerabilities that are applicable to an attacker possessing a Basic attack potential and according to *[NDcPP SD]* appendix A.

The total test effort expended by the evaluators was 8.5 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The TOE samples used for testing were the Huawei WLAN AirEngine Series VRP software V200R022C10SPC100 running on hardware AirEngine 9700-M1, AirEngine 5761-21, and AirEngine 6760-51EI.

There are different hardware versions covered by the TOE. The evaluators demonstrated that the TOE variants used for testing represented all TOE configurations through an equivalency argumentation.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei WLAN AirEngine Series Product running VRP software V200R022C10SPC100.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Huawei WLAN AirEngine Series Product running VRP software V200R022C10SPC100, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of *[NDcPP]*. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'exact' conformance to the Protection Profile *[NDcPP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None

3 Security Target

The Huawei WLAN AirEngine Series Product running VRP software Security Target, Version 1.8, 08 November 2023 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security CEM Common Methodology for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
OS	Operating System
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report “Huawei AirEngine Series Product V200R022C10SPC100” – NDcPP , 22-RPT-682, Version 3.0, 09 November 2023
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP]	collaborative Protection Profile for Network Devices, Version 2.2e. 23 March 2020.
[ST]	Huawei WLAN AirEngine Series Product running VRP software Security Target, Version 1.8, 08 November 2023

(This is the end of this report.)