Certification Report

Huawei CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200

Sponsor and developer: ***Huawei Technologies Co., Ltd.***
Administration Building
Huawei Industrial Base,
Bantian, Longgang,
Shenzhen 518129
People's Republic of China

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

Report number:	**NSCIB-CC-0351836-CR**
Report version:	**1**
Project number:	**0351836**
Author(s):	**Andy Brown**
Date:	**14 February 2022**
Number of pages:	**13**
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 CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200. The developer of the Huawei CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200 is Huawei Technologies Co., Ltd. located in Shenzhen, People's Republic of China and they also act as the sponsor of the evaluation and. 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 the software running on the CE16800&CE8800&CE6800 series switches. The software running on the switches is denominated Versatile Routing Platform (VRP) developed by Huawei. VRP provides extensive security features, including different interfaces with according access levels for administrators, enforcing authentications prior to establishment of administrative sessions, auditing of security-relevant management activities.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft. The evaluation was completed on 14 February 2022 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 CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200, 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 CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200 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 EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

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 CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200 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
Software	CE16800_V300R021C00SPC200.cc	V300R021C00SPC200
	CE6800-8800_ V300R021C00SPC200.cc	V300R021C00SPC200
	CE6820_V300R021C00SPC200.cc	V300R021C00SPC200

To ensure secure usage a set of guidance documents is provided, together with the Huawei CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200. For details, see section 2.5 "Documentation" of this report.

2.2 Security Policy

The TOE provides the following security functionalities:

- 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.
- 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 configured 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 behaviour of and modify the behaviour of the function's 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-sharedkeys, 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:

  - 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.
- Trusted path and channels for device authentication:
  - The TOE supports the trusted connections using TLS for the communication with the audit (syslog) server.
- Trusted updates:
  - The TOE supports installation of software updates by administrators after a successful verification of their authenticity using secure and strong cryptographic algorithms based on digital signatures.

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 4.2 of the *[ST]*.

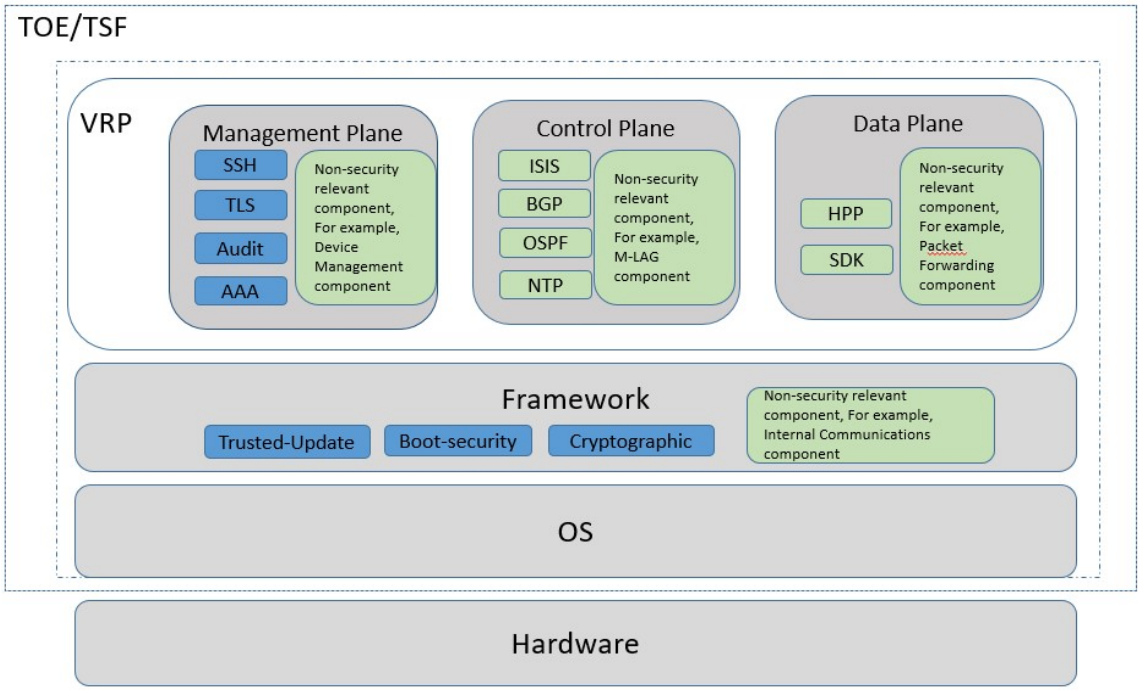
2.3.2 Clarification of scope

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 TOE is the software running on the CE16800&CE8800&CE6800 series switches. CE16800 is short for CloudEngine 16800. Other series switches are similar. These switches consist of both hardware (non-TOE) and software. The software running on the switches is denominated Versatile Routing Platform (VRP) developed by Huawei. VRP provides extensive security features, including different interfaces with according access levels for administrators, enforcing authentications prior to establishment of administrative sessions, auditing of security-relevant management activities.

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



The diagram above describes which modules of the VRP software are part of the TSF and which ones are not. Only the parts of the TOE highlighted in blue implement the SFRs.

2.5 Documentation

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

Identifier	Version
AGD_PRE Huawei CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200 Preparative Procedures	V08, 2021-1-21
AGD_OPE Huawei CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200 Operational User Guidance	V04, 2021-10-12
CloudEngine 8800 and 6800 V300R021C00 Upgrade Guide	V01, 2021-05-20
CloudEngine 16800 V300R021C00 Upgrade Guide	V01, 2021-05-20
CloudEngine 16800 Series Switches V300R021C00 Product Documentation	V03, 2021-11-10
CloudEngine 8800 and 6800 Series Switches V300R021C00 Product Documentation	V03, 2021-11-10

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

Extensive tests have been performed by the developer. The test cases were categorized based on SFR classes. The test cases were divided into seven chapters These test cases covered:

- All TSFIs
- All Subsystems and subsystem interactions

- Six chapters covered all the SFR classes:
  - FAU Class: 5 tests
  - FCS Class: 27tests
  - FIA Class:17 tests
  - FPTClass: 5 tests
  - FTP Class: 2 tests
  - FTA Class: 4 tests FMT Class 6tests
- One chapter mapped to additional tests for the SSH server and TLS client:
  - SSHS and TLSC tests: 4 tests

Since all SFRs were tested, the complete TSF was tested.

The evaluator repeated 8 of the developer test cases focussing on the TOE security mechanisms that were considered the most important including secure communication channels, password policies, audit log, session management and trusted update.

In addition to the developer testing, the evaluator derived and executed 13 independent functional security tests. The general strategy for defining the independent tests was:

- Extend the developer's test cases for crypto key management, authentication failure management, password management, and also complement the developer's test plan with additional negative test cases;
- Verify the AGD_PRE.1.2E activity (including the verification of integrity and authenticity of the TOE software steps);
- Verify TOE core management functionalities (such as authentication and logging);
- Scanning and fingerprinting for libraries/services searching for public known vulnerabilities to include in the vulnerability assessment;
- Verify TOE specific claims/security mechanisms (no access during TOE initialization, no action allowed before user authentication);
- Perform tests from the NDcPP that has not yet been covered by the developer.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered. During this examination several potential vulnerabilities were identified.
- Additional security analysis: When the implementation of the SFR was understood, a coverage check were performed on the relevant aspects of all SFRs. This expanded the listof potential vulnerabilities.
- Scanning the TOE using the applicable vulnerability scanning tools (e.g., NMAP, NESSUS) to collect information about the TOE and identify potential vulnerabilities.
- Public vulnerability search: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.
- The potential vulnerabilities identified were analyzed, and some of the potential vulnerabilities were concluded not exploitable within in the Enhanced-Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

The evaluator devised six (6) penetration tests to verify resistance to identified potential vulnerabilities.

The total test effort expended by the evaluators was 3 man days. During that test campaign, 100% of the time was spent on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*. Not all platforms were used for all the testing. Equivalency between platforms was established during the evaluation process. This enabled representative platforms to be used for testing and results to be considered to be applicable for all platforms used by the TOE.

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 has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 1 site certificate.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for the site(s) *[STAR]* [2].

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

Based on the above evaluation results the evaluation lab concluded the Huawei CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

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.

---

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

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 CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200 Security Target, Version 2.1, 21 January 2022 *[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:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
SSH	Secure Shell
TLS	Transport Layer Security
TOE	Target of Evaluation
UI	User Interface
VRP	Versatile Routing Platform

5 Bibliography

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

[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 CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200” – EAL4+, 21-RPT-893, Version 2.0, 01 February 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Huawei CE16800&CE8800&CE6800 Series Switches running VRP software V300R021C00SPC200 Security Target, Version 2.1, 21 January 2022.
[STAR-SUZ]	Site Technical Audit Report Huawei Suzhou R&D site, 21-RPT-826, Version 1.0, 17 January 2022.
[STAR-LAN]	Site Technical Audit Report Huawei Langfang Data Center, 21-RPT-1123, Version 1.0, 17 January 2022.

(This is the end of this report.)