Certification Report

Huawei NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500

Sponsor and developer: ***HUAWEI Technologies Co., Ltd.***
Administration Building, Huawei Base,
Bantian, Longgang District, Shenzhen 518129
China

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-217431-CR**

Report version: **1**

Project number: **217431**

Author(s): **Denise Cater**

Date: **12 April 2019**

Number of pages: **11**

Number of appendices: **0**

Headoffice:
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 Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-19-217431**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**HUAWEI Technologies Co., Ltd.** **Administration Building, Huawei Base, Bantian, Longgang District, Shenzhen 518129, China**
Product and assurance level	**Huawei NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500** Assurance Package: ▪ EAL2 augmented with ALC_FLR.2
Project number	**217431**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL4

Validity	Date of 1st issue : **17-04-2019** Certificate expiry : **17-04-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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 license 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, in order 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

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Huawei NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500. The developer of the Huawei NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500 is HUAWEI Technologies Co., Ltd. located in Shenzhen, 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 medium- or high-end network product developed by Huawei for transportation, finance, energy, government, education, enterprise, and Internet service provider (ISP) networks.

The NE20E series routers mainly serve as aggregation nodes on wide area networks (WANs) and egress nodes on enterprise or campus networks. They can be deployed at the access and aggregation layer of IP/MPLS networks.

The NE08E adopts an advanced routing architecture and a uniform platform to receive, transmit, and bear multiple types of services on an all-IP network. This helps construct reliable carrier-class packet transport networks (PTNs).

The NE20E series and NE08E series routers run on the Versatile Routing Platform (VRP) operating system and use Huawei-developed NP chips and hardware-based forwarding and non-blocking switching technologies. VRP features include assigning different privileges to administration users with different privilege levels; enforcing authentications prior to establishment of administrative sessions with the TOE; auditing of security-relevant management activities; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 11 April 2019 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 NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500, 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 NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500 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 EAL2 augmented (EAL2(+)) 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]*.

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. It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Huawei NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500 from HUAWEI Technologies Co., Ltd. located in Shenzhen, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NE20E-S8A	See *[ST] Table 2 and Table 3* for list of boards and versions
	NE20E-S16A	
	NE08E-S6E	See *[ST] Table 4* for list of boards and versions
Software	NE20E series Router V800R010C10SPC500	V800R010C10SPC500
	NE08E series Router V300R003C10SPC500	V300R003C10SPC500

To ensure secure usage a set of guidance documents is provided together with the Huawei NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500. Details can be found in section ”Documentation” of this report.

2.2 Security Policy

The “security policy” of the TOE is defined by the SFRs, which are defined in [ST] Section 6.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in 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 components of the TOE are identified in [ST] Section 1.4.

2.5 Documentation

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

Identifier	Version
HUAWEI NE20E&NE08E Common Criteria Security Evaluation - Certified Configuration	Version 2.1, dated 2019-03-25
NE20E V800R010C10 Product Documentation 01	V800R010C10,

	dated 2018-04-30
NE08E V300R003C10 Product Documentation 01	V300R003C10, dated 2018-04-30

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

The developer test plan consists of 12 different categories of tests of 90 tests. The categories are based on groupings of major security functionalities, and, in combination with all SFRs and TSFIs. In addition, the developer also performed a number of penetration tests to demonstrate the TOE is resistant against common attacks of the switch/router TOE type.

For the testing performed by the evaluators, the developer provided a test environment. The evaluators have reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator. A total of 8 developer tests were selected and repeated. All test cases were performed on the NE20E device, with 2 of them also performed on the NE08E. In addition, the evaluator devised 11 independent functional test cases, the execution of which led to one additional test case resulting in total of 12 independent functional test cases tests being executed by the evaluator.

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 checks were performed on the relevant aspects of all SFRs. This expanded the list of 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 analysed, and some of the potential vulnerabilities were concluded not exploit within in the Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, 14 penetration tests were devised:

Penetration test category	Number of tests	Test Executed on
Router attacks/vulnerabilities	4	All on NE20E only
Management Plane	4	3 on both NE20E & NE08E 1 on NE08E only
Data plane attacks/vulnerabilities	6	3 on NE20E 3 on NE08E

2.6.3 Test Configuration

The TOE was tested in the following configurations:

- NE08E device running V300R003C10SPC500
  - NE08 S6E with MPU-A with 8 ports 100/1000 SFP line card
- NE20E device running V800R010C10SPC500
  - NE20E S16A with MPU-E1 and NSP-B with 10 ports 100/1000 SFP line card

2.6.4 Testing 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.

2.7 Re-used evaluation results

None.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] 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 NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500, to be CC Part 2 conformant, CC Part 3 conformant, and to meet the requirements of **EAL 2 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 contains necessary information about the usage of the TOE.

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

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

3 Security Target

The HUAWEI NE20E series Router V800R010C10 & NE08E series Router V300R003C10 Security Target v3.0, 2019-04-08 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

ISP	Internet Service Provider
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
PTN	Packet Transport Networks
TOE	Target of Evaluation
VRP	Versatile Routing Platform
WAN	Wide Area Networks

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 NE20E Router V800R010C10 and NE08E Router V300R003C10, revision SPC500, 19-RPT-206, Version 3.0, 11 April 2019.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.
[ST]	HUAWEI NE20E series Router V800R010C10 & NE08E series Router V300R003C10 Security Target v3.0, 2019-04-08.

(This is the end of this report).