Certification Report

Huawei NetEngine 8000 Series Routers' Software V800R012C10, patch version V800R012C10SPC300

Sponsor and developer:	***Huawei Technologies Co., Ltd.*** **Huawei Base, Bantian, Longgang District,** **Shenzhen, China.**
Evaluation facility:	***Riscure B.V.*** **Delftechpark 49** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-0207368-CR**
Report version:	**1**
Project number:	**0207368**
Author(s):	**Andy Brown**
Date:	**01 September 2021**
Number of pages:	**12**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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 NetEngine 8000 Series Routers' Software V800R012C10, patch version V800R012C10SPC300. The developer of the Huawei NetEngine 8000 Series Routers' Software V800R012C10, patch version V800R012C10SPC300 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 software running on the NetEngine 8000 series routers. It is defined as the software running on the hardware corresponding to the following Huawei routers: NetEngine 8000 F1A-8H20Q, NetEngine 8000 M8, NetEngine 8000 M14, NetEngine 8000 X4 and NetEngine 8000 X8. These routers consist of both hardware (non-TOE) and software (TOE and non-TOE portions). The software running on the routers 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 software consists of TSF and non-TSF parts.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 01 September 2021 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 NetEngine 8000 Series Routers' Software V800R012C10, patch version V800R012C10SPC300, 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 NetEngine 8000 Series Routers' Software V800R012C10, patch version V800R012C10SPC300 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 *[ST]* includes Security Functional Requirements (SFR's) from the Collaborative Protection Profile for Network Devices, Version 2.1.

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 NetEngine 8000 Series Routers' Software V800R012C10, patch version V800R012C10SPC300 from Huawei Technologies Co., Ltd. located in Shenzhen, China.

The TOE is comprised of the following main components:

Delivery item type	**Identifier**	**Version**
Software	Huawei NetEngine 8000 Series Routers Software V800R012C10	V800R012C10SPC300

To ensure secure usage a set of guidance documents is provided, together with the Huawei NetEngine 8000 Series Routers' Software V800R012C10, patch version V800R012C10SPC300. 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
- Cryptographic support
- Identification and authentication
- Secure Management
- Protection of the TSF
- TOE access through user authentication
- Trusted path and channels for device authentication
- Trusted software updates

These features are explained in detail in Section 1.4.2 of the security target. In addition, the description references the main modules used to enforce security and to supply the server infrastructure. Modules here refer to software subsystems within the TOE. They are:

- AAA (Authentication Authorization Accounting)
- SSH
- Cryptographic
- Audit
- NTP
- Boot-Security
- Trusted-Update
- TLS

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

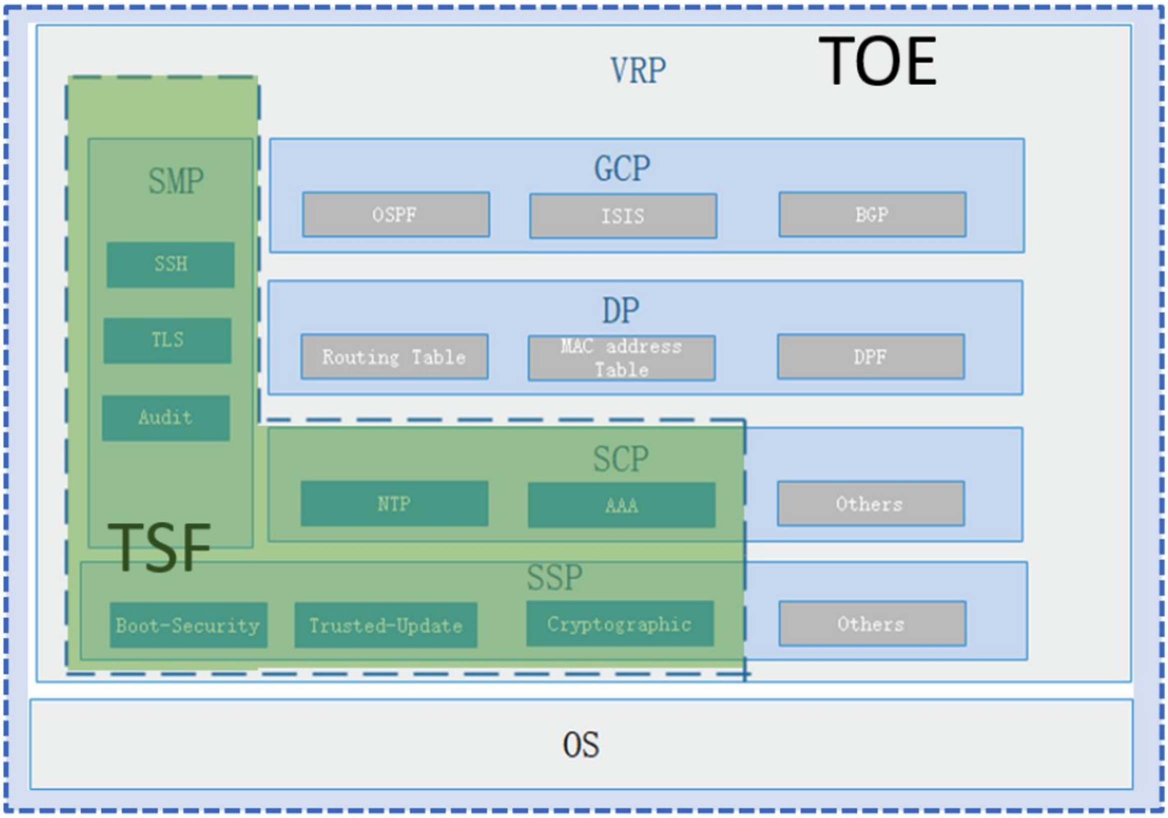
The TOE scope consists of the software running in the router device. The hardware is out of TOE scope.

The underlying OS on which the TOE software is supported consists in a Linux operating system. The OS provides basic services including memory management, scheduling management, file management, and device management.

The VRP software is a network operating platform, which has a distributed, multi-process, and component-based architecture. It builds upon the hardware development trend and will meet carriers' exploding service requirements.

The VRP software is responsible for functional management, routing information generation, receiving generated routing information and formatting them into hardware-specific data to direct traffic forwarding.

The diagram below describes which modules of the VRP software are part of the TSF and which ones are not. Only the part of the TOE highlighted in green is included in the TSF.



Architecture and boundaries of the Target of Evaluation

VRP consists of SMP, SCP, GCP, DP and SSP. Only SMP, SCP and SSP are in the scope of the TSF. OS, GCP and DP are not in the scope of the TSF.

6 logical planes are defined for the Software Architecture, they are:

- In TSF scope:
  - System Manage Plane (SMP), implements management for external access, management for system configuration, information output on VRP;

  - Service Control Plane (SCP), implements authentication, authorization, accounting and other serviceable functionality on VRP;
  - System Service Plane (SSP), implements system internal scheduling, communication, management of signals, events, timers, etc. System security functions are also implemented at this plane.
- Out of TSF scope:
  - General Control Plane (GCP), implements routing information learning, ARP table entry learning, STP (Spanning Tree Protocol) topology management, and functionalities related to TCP/IP stack on VRP;
  - Data Plane (DP), implements traffic forwarding. Forwarding related information, e.g. routing information, ARP table entry, static MAC table entries are generated in GCP and downloaded via communication channel provided by SSP;
  - Operating System (OS), provides hardware and software resource management.

2.5 Documentation

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

Identifier	Version
AGD_PRE Huawei NetEngine 8000 Series Routers' VRP Software V800R012C10 Preparative Procedures	10.0
AGD_OPE Huawei NetEngine 8000 Series Routers' VRP Software V800R012C10 Operational User Guidance	9.0
NetEngine 8000 X4X8 V800R012C10SPC300 Upgrade Guide	1.0
HUAWEI NetEngine 8000 M14 and M8 Product Documentation	03, 2020-10-31

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 evaluator made a sampling of the developer test cases based on the following criteria:

- Tests covering TSFIs exposed to the Internet
- Tests covering privilege separation
- Tests covering authentication.

Since this was a device designed to be connected to the Internet, the evaluator focused on test cases that would result in an attacker gaining administrative control of the TOE.

The evaluator repeated 4 of the developer’s test cases.

In addition, the evaluator devised 1 additional independent functional test to further complement the coverage.

2.6.2 Independent penetration testing

The TOE is a network server that performs routing. Therefore, the vulnerability analysis was conducted using the network attack methods, and is structured in the following phases:

- Information Gathering and Potential Vulnerability Identification: understand network structures, server properties using port scanning, detection of running services etc. and conducting public vulnerability searches to identify potential vulnerabilities

- Exploitation: get some first unprivileged access e.g. by manipulating file upload mechanisms, authentication bypass, password attacks etc.
- Privilege escalation: escalate to extended / root privileges to gather further information on operating system properties, application services, file-system structures to get deeper into the system and break security features

The vulnerability analysis took information from the design assessment of the TOE into account. The ADV/ATE documentation along with the source code review that was done as part of the combined AVA/ADV_IMP assessment also provided insight into areas that could be potentially vulnerable. These were then testing in the penetration testing phase.

To rate the difficulties to exploit potential vulnerabilities the evaluator used the standard rating methodology from the Common Criteria Standard. The reason for this choice was that the standard rating focusses on the efforts of creating / identifying a potential exploit which was the most important factor as exploits for this type of product usually have to be deployed remotely and therefore scale quite well. Thus, there was no reason for applying a specific rating scheme which for example explicitly splits identification and exploitation efforts.

The evaluator performed 4 penetration tests. The total test effort expended by the evaluators was 1.5 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 V800R012C10SPC300 software running on NetEngine 8000 M14 hardware.

The samples were delivered by the developer in a state that was not the certified configuration. The evaluator followed the preparation guidance identified in section 2.5 to configure the TOE in the certified configuration. The developer also provided a configuration file to configure the TOE.

There are different hardware versions supported by the TOE, however the difference between the various versions is the number of interfaces each offers. Therefore the version of the hardware that was available for testing (NetEngine 8000 M14) is representative of the other hardware versions within the context of this evaluation.

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.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei NetEngine 8000 Series Routers’ Software V800R012C10, patch version V800R012C10SPC300.

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 NetEngine 8000 Series Routers’ Software V800R012C10, patch version V800R012C10SPC300, 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.

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 NetEngine 8000 Series Routers' Software Security Target, Version 1.1, 28 August 2021 *[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
DP	Data Plane
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCP	General Control Plane
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
SCP	Service Control Plane
SMP	System Manage Plane
SSH	Secure Shell
SSP	System Service Plane
TOE	Target of Evaluation
VRP	Versatile Routing Platform

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 for Huawei NetEngine 8000 Series Routers Software v800R012C10, 20200131-D8, Version 1.3, 30 August 2021
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Huawei NetEngine 8000 Series Routers' Software Security Target, Version 1.1, 28 August 2021

(This is the end of this report.)