Certification Report

Huawei server management software iBMC V662/V3.01.12.02

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

Evaluation facility: ***Riscure***
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-0176341-CR**
Report version:	**1**
Project number:	**0176341**
Author(s):	**Andy Brown**
Date:	**26 October 2020**
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

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 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 server management software iBMC V662/V3.01.12.02. The developer of the Huawei server management software iBMC V662/V3.01.12.02 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.

Huawei Server management software iBMC is an embedded server management system that is used to manage servers throughout their lifecycle. It provides a series of management tools for hardware status monitoring, energy savings, and security protection. It adopts standard interfaces to build a comprehensive ecosystem for server management.

Huawei Server management software iBMC implements various remote operation and maintenance (O&M) tools and capabilities. It supports remote configuration, power consumption management, fault diagnosis and fault management, allowing O&M personnel to conveniently access servers and perform configuration, management and recovery.

Huawei Server management software iBMC can be widely used in Huawei servers for any server use-case, such as servers in data center.

The TOE consists of a software meant to be deployed on a supporting hardware (Hi1710 or Hi1711) which is not in the scope of the evaluation.

The main security service provided by the TOE is the protection of the remote management interfaces including communication security, authentication and authorization access controls, and the audit / logging of security relevant events.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 26 October 2020 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 server management software iBMC V662/V3.01.12.02, 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 server management software iBMC V662/V3.01.12.02 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 provides sufficient evidence that the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC FLR.1 (Basic flaw remediation).

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 server management software iBMC V662/V3.01.12.02 from Huawei Technologies Co., Ltd. located in Shenzhen, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	iBMC-V662.zip	V662
	iBMC-V3.01.12.02.zip	V3.01.12.02
Software signature file	iBMC-V662.zip.asc	N/A
	iBMC-V3.01.12.02.zip.asc	N/A

To ensure secure usage a set of guidance documents is provided together with the Huawei server management software iBMC V662/V3.01.12.02. Details can be found in section 2.5 of this report.

Since the evaluation is an EAL2 evaluation augmented by ALC_FLR.1, the life-cycle definition (ALC_LCD) was not in the scope and has not been assessed.

2.2 Security Policy

The TOE provides all the following main security features:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Functionality Management • TOE Access
- Trusted Path/Channel

The protocol security to protect the communication is based on the following protocols:

- SSHv2 for an access through the CLI interface
- TLS for an access through Redfish and WebUI interfaces
- Syslog and NTP interfaces are not externally accessible but may be configured to secure the communication with the Syslog and NTP servers; the evaluation assumes that these servers are located in the same secured areas than the iBMC server
- Other interfaces and associated protocols are out of scope of the evaluation

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 TOE consists of the iBMC software. It runs on top of a hardware (Hi1710 or Hi1711).

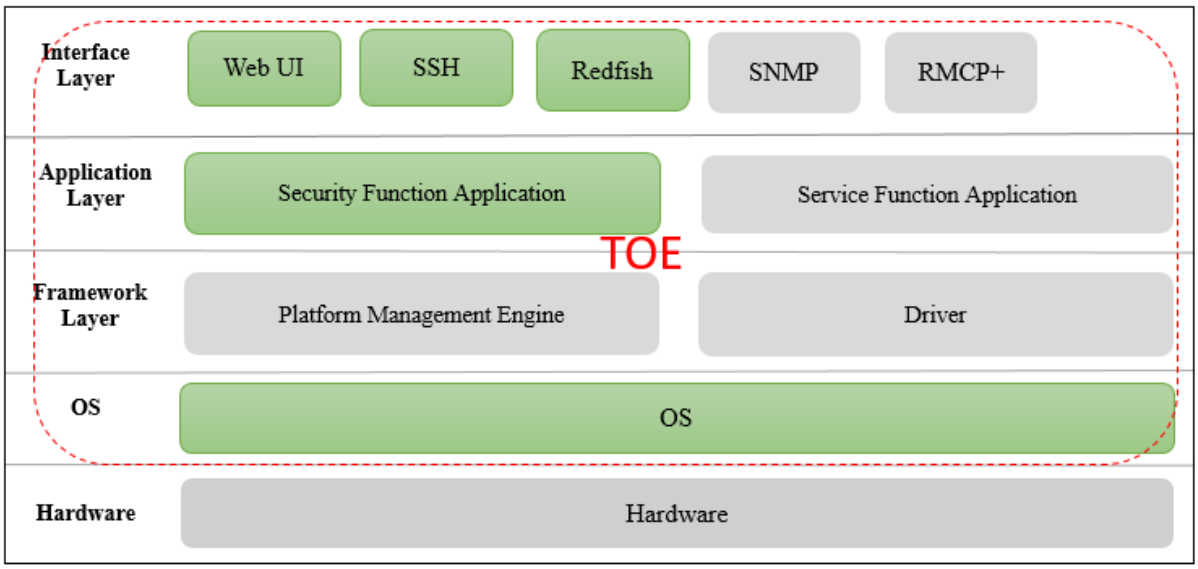

Figure 5.1: TOE Overview

The overview shows the technical implementation in a traditional layered representation. The TOE's software architecture consists several layers dedicated to hardware management, security functionalities management and interfaces management.

Huawei Server management software iBMC mainly implements monitoring, troubleshooting, power consumption management and remote operation and management. Huawei Server management software iBMC provides a WebUI, a Redfish interface and a SSH interface to the outside world. Other protocols such as SNMP and RMCP are disabled in the certified configuration. The security function application manages authentication and identification of external user connecting to the TOE through a management terminal. After authentication and identification, requests received are executed by the Interface and Application layers, making use of services provided by the OS layer.

2.5 Documentation

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

Identifier	Version
Huawei Technologies Co.,Ltd., Huawei Server Management Software iBMC AGD_PRE_User	V1.5
Huawei Technologies Co.,Ltd., Huawei Server Management Software iBMC AGD_PRE_Production	V1.4
Huawei Technologies Co.,Ltd., Huawei Server Management Software iBMC AGD_OPE	V1.5

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 devised 43 test cases providing evidence of coverage for the security functionality. The evaluator sampled 4 of these developer tests. The rationale for choosing those tests is the complexity,

the number of threats the tests are addressing, and also the number of interfaces that the tests are using.

In addition, the evaluator devised 3 additional independent evaluator tests to further complement the coverage.

2.6.2 Independent Penetration Testing

The TOE is a server-based solution. Therefore, the vulnerability analysis is conducted using the network attack methods, as for example covered in the Offensive Security Certified Professional program, 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, SQL injections, password attacks, cross-site scripting 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 takes information from the design assessment of the TOE into account. However, an EAL2 evaluation is more explorative in nature than a full white-box evaluation where also implementation details and source code are available for inspection, so specific emphasis is placed upon the information gathering activities.

To rate the difficulties to exploit potential vulnerabilities the evaluation uses the standard rating methodology from the Common Criteria Standard [CCDBMB.CCP3]. The reason for this choice is that the standard rating focusses on the efforts of creating / identifying a potential exploit which is the most important factor as exploits for this type of products usually have to be deployed remotely and therefore scale quite well. Thus, there is no reason for applying a specific rating scheme which for example explicitly splits identification and exploitation efforts.

2.6.3 Test Configuration

Two instances of the TOE were provided by the developper:

- A server running iBMC v662 (product name Huawei 2288 V5)
- A server running iBMC v3.01.12.02 (product name Huawei TaiShan 200)

A single instance of the TOE was used for remote testing, the Huawei TaiShan 200 server running iBMC version 3.01.12.02. In the discovery phase part of the Vulnerability analysis was conducted on both servers provided. No discrepancies were found.

In addition, the witnessing session performed as part of ALC_CMS allowed the assessment of the differences between v662 and v3.01.12.02 of iBMC. It was concluded that the testing performed on v3.01.12.02 also valid on v662 of iBMC.

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

There is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei server management software iBMC V662/V3.01.12.02. A user can identify the TOE using the WebUI, as the version is displayed on the Home page. Alternatively, the CLI command ipmcget -d version may be used to identify the TOE. These identification methods are described in section 4.1.2 of [AGD_OPE].

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*.

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

Based on the above evaluation results the evaluation lab concluded the Huawei server management software iBMC V662/V3.01.12.02, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 2** augmented with ALC_FLR.1. 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. The TOE needs to be operated in a segregated network that only allows for access via the remote interfaces and by physically protected interfaces (OE.NetworkSegration and OE.PhysicalProtection). Personnel working as authorized administrators are expected to be carefully selected for trustworthiness and trained for proper operation of the TOE (OE.NoEvil). Also note that the certified configuration is limited to a specified TLS 1.2 cipher suites.

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

3 Security Target

The CC Security Target for Huawei Server Management Software iBMC, Issue 1.8, 2020-08-03 *[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:

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
PP	Protection Profile
SSH	Secure Shell
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 server management software iBMC V662/V3.01.12.02, 20200075-D3, Version 1.1, 20 October 2020.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[ST] CC Security Target for Huawei Server Management Software iBMC, Issue 1.8, 2020-08-03.

(This is the end of this report).