TÜV Rheinland Nederland B.V.

Certification Report

xFusion Server intelligent Baseboard Management Controller iBMC version 3.3.10.7

Sponsor and developer:	***xFusion Digital Technologies Co., Ltd*** **Building 1, Zensun Boya Square, Longzihu Wisdom Island** **Zhengdong New District 450046, Zhengzhou, Henan** **Province, People's Republic of China**
Evaluation facility:	***UL*** **De Heyderweg, 2** **Leiden, 2314XZ** **The Netherlands**
Report number:	**NSCIB-CC-0573644-CR**
Report version:	**1**
Project number:	**0573644**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**28 Febuary 2023**
Number of pages:	**11**
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 xFusion Server intelligent Baseboard Management Controller iBMC version 3.3.10.7. The developer of the xFusion Server intelligent Baseboard Management Controller iBMC version 3.3.10.7 is xFusion Digital Technologies Co., Ltd located in Zhengzhou, Henan Province, P.R.C. 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.

xFusion Server intelligent Baseboard Management Controller iBMC is an out of band management system optimized for server remote management. It consists of hardware and firmware embedded on the motherboard of xFusion server, and independent to in-band components such as host processors, OS, storages, etc., so that the server can be managed without relying on the status of the in-band components, and the management operation will not interfere with services run on the server.

The TOE is the firmware executed on the Management Plane of the supported xFusion servers, providing server management functionalities.

The TOE has been evaluated by UL located in Leiden, The Netherlands. The evaluation was completed on 23 February 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 xFusion Server intelligent Baseboard Management Controller iBMC version 3.3.10.7, 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 xFusion Server intelligent Baseboard Management Controller iBMC version 3.3.10.7 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.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]* (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 xFusion Server intelligent Baseboard Management Controller iBMC version 3.3.10.7 from xFusion Digital Technologies Co., Ltd located in Zhengzhou, Henan Province, P.R.C.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Firmware	xFusion Server intelligent Baseboard Management Controller iBMC	3.3.10.7

The xFusion server models that support the TOE are:

FusionServer	1288H V6, 2288H V6, 2488H V6, 5288 V6, XH321 V6, XH321C V6, 1288H V7, 2288H V7, 5885H V7, 5288 V7, XH321 V7, XH321C V7, G5500 V7, G8600 V7, 5298 V7
FusionPoD	DA140C V2, DH140C V6, DH120C V6, DA126C V2, DA120C V2, DA120 V2, RM210, DH122C V6, DH141C V6, DH120C V7, DH141C V7

To ensure secure usage a set of guidance documents is provided, together with the xFusion Server intelligent Baseboard Management Controller iBMC version 3.3.10.7. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE provides the following security functionality:

- Identification and Authentication
- Authorization
- Security Audit
- Cryptographic Support
- Security Management
- TOE access
- Trusted communication
- Secure updating
- Secure booting

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

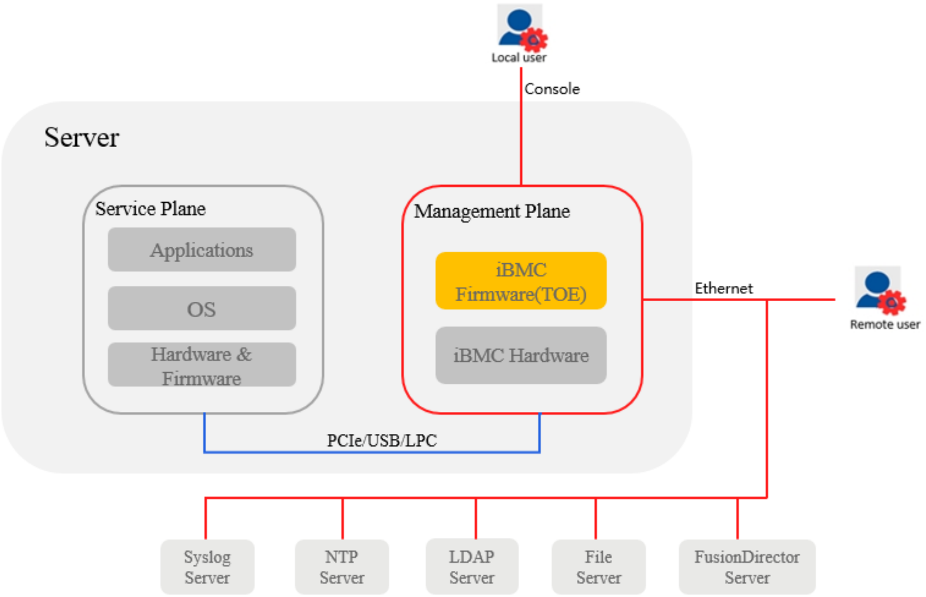
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 3.5 of the *[ST]*.

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 constitutes of the firmware executing on the management plane which is hosted by the xFusion server, the server itself including its service plane is out of the TOE scope.



The TOE is comprised of the following subsystems:

Interface Management Subsystem This subsystem implements all application layer interfaces management, including security functional interfaces and service functional interfaces.

System Management Subsystem This subsystem implements most of BMC security functionalities, which may rely on platform functions provided by the OS subsystem, and may be called by IM to perform or manage security functions.

Operating System Subsystem This subsystem including underlying OS and other platform modules which provide fundamental functionalities to support BMC running.

Secure Booting and Secure Updating Subsystem Initial booting program part of the root of trust, verification of L1FW, load and verify other firmware's which will be executed later (uboot, rootfs and the host server BIOS) and check if there's firmware update or not.

2.5 Documentation

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

Identifier	Version
xFusion Server intelligent Baseboard Management Controller iBMC EAL4+ AGD_OPE_V1.5	1.5
xFusion Server intelligent Baseboard Management Controller iBMC EAL4+ AGD_PRE_Production_V1.1	1.1
xFusion Server intelligent Baseboard Management Controller iBMC EAL4+ AGD_PRE_User_V1.5	1.5

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 performed comprehensive testing on functional specification and subsystem level. These tests are grouped by the security functions: Identification and Authentication, Authorization, Security Audit, Cryptographic Support, Security Management, TOE access security, Trusted Communications, Secure Booting and Secure Updating.

The evaluator selected a sample of the developer test cases to repeat. The selected sample exercised all TSFIs and subsystems of the TOE.

The evaluator created additional test cases test to supplement coverage of SFRs, TSFI and subsystem interactions. These test cases were also developed to further exercise the behaviour of critical functionality.

2.6.2 Independent penetration testing

The independent vulnerability analysis consisted of two main components:

- Analysis of the implementation of the security architecture, including:
    - Secure initialization of the TOE
    - Tamper resistance of the TOE
    - Non-bypassability of the TSF
    - Exception handling by the TOE
- Analysis of the implementation of each of the SFRs from the ST

From the analysis, a number of areas of concern were identified, which were further investigated through penetration testing. The penetration testing demonstrated that the TOE was resistant to attacks from an attacker with enhanced-basic attack potential.

The total test effort expended by the evaluators was 30 days. During that test campaign, 100% of the total 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]*.

The testing of the TOE firmware was performed using the TOE installed on a FusionServer 2288H V6.

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.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number xFusion Server intelligent Baseboard Management Controller iBMC version 3.3.10.7.

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 xFusion Server intelligent Baseboard Management Controller iBMC version 3.3.10.7, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 4 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 "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 xFusion Server intelligent Baseboard Management Controller iBMC CC EAL4+ Security Target, Version 2.0, 02 Febuary 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:

iBMC	intelligent Baseboard Management Controller
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LDAP	Lightweight Directory Access Protocol
NSCIB	Netherlands Scheme for Certification in the area of IT Security
NTP	Network Time Protocol
TOE	Target of Evaluation
UL	Underwriters Laboratories Inc.

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]	xFusion Server intelligent Baseboard Management Controller iBMC Evaluation Technical Report, UL14273557/ETR, Version. 1.0, 23 February 2023
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	xFusion Server intelligent Baseboard Management Controller iBMC CC EAL4+ Security Target, Version 2.0, 02 Febuary 2023

(This is the end of this report.)