Reference: 2023-25-INF-4631- v1
Target: Limitada al expediente
Date: 26.01.2026

Created by: I007
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2023-25**
TOE	**iMC MagicBox (iMC PLAT, iMC EIA) version 7.3 (PLAT E0708P13, EIA E0629)**
Applicant	**91330100754408889H - New H3C Technologies Co., Ltd.**

References

[EXT-8657] Certification Request

[EXT-8657] 2023-07-07_2023-25_certification_request

[EXT-8657] 2023-07-07_2023-25_certification_request

[EXT-8657602] 2023-07-07_2023-25_certification_request

[EXT-8657603] 2023-07-07_2023-25_certification_request

[EXT-8657604] 2023-07-07_2023-25_certification_request

[EXT-8657605] 2023-07-07_2023-25_certification_request

[EXT-8657606] 2023-07-07_2023-25_certification_request

[EXT-8657607] 2023-07-07_2023-25_certification_request

Certification report of the product iMC MagicBox (iMC PLAT, iMC EIA) version 7.3 (PLAT E0708P13, EIA E0629), as requested in [EXT-8657] dated 07/07/2023, and evaluated by SGS Brightsight Barcelona, S.L. (Unipersonal), as detailed in the Evaluation Technical Report [EXT-9709] received on 22/07/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product iMC MagicBox (iMC PLAT, iMC EIA) version 7.3 (PLAT E0708P13, EIA E0629).

The TOE is network management device providing role and device-based network access control for employees, contractors and guests across any wired, wireless and VPN infrastructure. iMC implements profiling, guest access, and health checks, facilitating centralized management of network access policies. iMC provides user and device authentication based on 802.1X, non-802.1X and web portal access methods.

Developer/manufacturer: New H3C Technologies Co., Ltd.

Sponsor: New H3C Technologies Co., Ltd..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: SGS Brightsight Barcelona, S.L. (Unipersonal).

Protection Profile: collaborative Protection Profile for Network Devices, v.2.2e, 2020-03-23.

Evaluation Level: Common Criteria v3.1 R5 EAL1 + ASE_SPD.1 (defined by Protection Profile).

Evaluation end date: 29/07/2025

Expiration Date[1]: 4/11/2030

All the assurance components required by the evaluation level EAL1 (augmented with ASE_SPD.1) have been assigned a “PASS” verdict. Consequently, the laboratory SGS Brightsight Barcelona, S.L. (Unipersonal) assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL 1 + ASE_SPD.1, as defined by the Common Criteria v3.1 R5, the CEM v3.1 R5 and the collaborative Protection Profile for Network Devices, v.2.2e, 2020-03-23.

Considering the obtained evidences during the instruction of the certification request of the product iMC MagicBox (iMC PLAT, iMC EIA) version 7.3 (PLAT E0708P13, EIA E0629), a positive resolution is proposed.

TOE SUMMARY

H3C iMC MagicBox consists of one platform (iMC PLAT) and one component (iMC EIA):

iMC PLAT consists of a base platform for delivering network resource management capabilities and optional service modules for extending iMC’s functionality. The base platform provides

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

administrators and operators with the basic and advanced functionality needed to manage iMC and the devices, users, and services managed by iMC. The base platform incorporates the essential functional areas of network management – fault, configuration, asset management and auditing, performance, and security.

The iMC is a network management system, iMC is located at the management and control layer of the network, it can manage and control various network devices, including switches and routers. It provides open interface to quickly integrate with upper-layer application systems such as OSSs, service orchestrators and service application.

For the iMC architecture, in the northbound direction, it provides Web portals and northbound interfaces for O&M personnel, OSS. In the southbound, it provides configuration and management capabilities for H3C network devices and third-party network elements.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL1 and the evidences required by the additional component ASE_SPD.1, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_FSP.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.1
	ALC_CMS.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.1
	ASE_REQ.1
	ASE_TSS.1
	ASE_SPD.1
ATE	ATE_IND.1
AVA	AVA_VAN.1

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

- FAU_GEN.1 Audit Data Generation
- FAU_GEN.2 User identity association
- FAU_STG_EXT.1 Protected Audit Event Storage
- FAU_STG.1 Protected Audit Trail Storage
- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- FCS_CKM.4 Cryptographic Key Destruction
- FCS_COP.1/DataEncryption Cryptographic operation (AES Data Encryption/Decryption)
- FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)
- FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)
- FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)
- FCS_RBG_EXT.1 Random Bit Generation
- FCS_HTTPS_EXT.1 HTTPS Protocol
- FCS_SSHC_EXT.1 SSH Client Protocol
- FCS_SSHS_EXT.1 SSH Server Protocol
- FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication
- FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication
- FIA_AFL.1 Authentication Failure Management
- FIA_PMG_EXT.1 Password Management
- FIA_UIA_EXT.1 User Identification and Authentication
- FIA_UAU_EXT.2 Password-based Authentication Mechanism
- FIA_UAU.7 Protected Authentication Feedback
- FIA_X509_EXT.1 X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication
- FMT_MOF.1/ManualUpdate Management of Security Functions Behaviour

- FMT_MOF.1/Services Management of Security Functions Behaviour
- FMT_MTD.1/CoreData Management of TSF Data
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.2 Restrictions on security roles
- FPT_SKP_EXT.1 Protection of TSF Data
- FPT_APW_EXT.1 Protection of Administrator Passwords
- FPT_TST_EXT.1 TSF Testing (Extended)
- FPT_TUD_EXT.1 Trusted Update
- FPT_STM_EXT.1 Reliable Time Stamps
- FTA_SSL_EXT.1 TSF-initiated Session Locking
- FTA_SSL.3 TSF-initiated Termination
- FTA_SSL.4 User-initiated Termination
- FTA_TAB.1 Default TOE Access Banners
- FTP_ITC.1 Inter-TSF Trusted Channel
- FTP_ITC.1 Inter-TSF Trusted Channel

IDENTIFICATION

Product: iMC MagicBox (iMC PLAT, iMC EIA) version 7.3 (PLAT E0708P13, EIA E0629)

Security Target: *iMC MagicBox - Security Target, v3.4, 2025-07-08*.

Protection Profile: collaborative Protection Profile for Network Devices, v.2.2e, 2020-03-23.

Evaluation Level: Common Criteria v3.1 R5 EAL1 + ASE_SPD.1 (defined by Protection Profile).

SECURITY POLICIES

The use of the product iMC MagicBox (iMC PLAT, iMC EIA) version 7.3 (PLAT E0708P13, EIA E0629) shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 3 (“Security Problem Definition”), pointing out to the section 4.3 (“Organizational Security Policy”) of the [PP-ND].

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 3 ("Security Problem Definition"), pointing out to the section 4.2 ("Assumptions") of the [PP-ND].

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product iMC MagicBox (iMC PLAT, iMC EIA) version 7.3 (PLAT E0708P13, EIA E0629), although the agents implementing attacks have the attack potential according to the AVA_VAN.1 of EAL1 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 3 ("Security Problem Definition"), pointing out to the section 4.1 ("Threats") of the [PP-ND].

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 ("Security Objectives for the operational Environment").

ARCHITECTURE

LOGICAL ARCHITECTURE

Security audit

The TOE generates audit records for security-relevant management and stores the records in the database. Operation logs record operation events of the TOE, logs can record operator name, IP address, component name, operation time, operation and result. The query and filter functions are provided on the iMC GUI, which allows authorized users to search audit logs.

Cryptographic support

The TOE generates audit records for security-relevant management and stores the records in the database. Operation logs record operation events of the TOE, logs can record operator name, IP address, component name, operation time, operation and result. The query and filter functions are provided on the iMC GUI, which allows authorized users to search audit logs.

Identification and authentication

The TOE authenticates all users who access the TOE by user name and password.

Security management

The TOE offers security management for all management aspects of the TOE. Security management includes not only authentication and access control management, but also management of security-related data consisting of configuration profiles and runtime parameters.

Protection of the TSF

TOE saves all of TSF data in the database, and user cannot read them on the iMC GUI. iMC is deployed on the MagicBox, VM and physical server, only the server administrator can query the version of software and update it.

TOE access

TOE is able to configure the operator idle timeout parameter, default 30 mins. User will be automatically offline after exceeding the set operator idle timeout. The administrator can force users to offline.

Trusted path/channels

The TOE supports encrypted transmission within the iMC MagicBox server, between devices and the iMC Magic Box server, between browser and the iMC MagicBox server, between syslog server and the iMC MagicBox server and between OSS/third-party application and the iMC MagicBox server.

PHYSICAL ARCHITECTURE

Appliance Model	Component	CPU
H3C iMC MagicBox 2000	*iMC PLAT, iMC EIA*	*Intel XeonI E5-2620V4, 8 Cores*

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

[AGD_PRE]	Preparative and Operative Procedures for CC NDPP iMC Magicbox v1.4, 2024-09-18
[IMC_ADM_GUIDE]	H3C iMC Enterprise and Standard Platform Administrator Guide-7.3, 5W112
[IMC_INST_GUIDE]	H3C iMC MagicBox Installation Guide-7.3, 5W102
[IMC_USER_GUIDE]	H3C iMC User Access Manager Administrator Guide-7.3, 5W108
[IMC_UAM_CERT]	H3C iMC UAM Configuration Examples, 5PW103
[IMC_TAM_CERT]	H3C iMC TAM Configuration Examples, 5PW100
[IMC_PLAT_TRU]	H3C IMC PLAT Troubleshooting Guide, 5PW104
[IMC_UAM_TRU]	H3C iMC UAM Troubleshooting Guide, 5PW102
[IMC_PLAT_CERT]	H3C iMC PLAT Configuration Examples, 5W108
[IMC][ADV]	H3C iMC MagicBox - Functional Specification v2.2, 2024-07-10
[IMC][DAR]	H3C iMC MagicBox-DAR v0.2, 2024-07-04

PRODUCT TESTING

Regarding the ATE testing, the evaluator followed the approach described in the [PP-ND] and [PP-ND-SUPPORT], the approach resulted on the 100% of the TSFI and the SFRs tested.

A “Flaw hypothesis methodology” has been executed to assess to devise the applicable potential vulnerabilities and generate a test plan. Common criteria Methodology [CEM] has been used to rate the attacks.

The attacks executed covers 100% of the TSFI and focusing in the known vulnerabilities and the common attacks.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated in the [ST], sections 1.3 (“TOE Overview”) and 1.4 (“TOE Description”). Therefore, for the operation of the product iMC MagicBox (iMC PLAT, iMC EIA) version 7.3 (PLAT E0708P13, EIA E0629) it is necessary the disposition of those components

The following configuration has been used on this evaluation:

- iMC MagicBox (iMC PLAT, iMC EIA) v7.3 in an appliance model H3c iMC.

The evaluator confirmed the correct version of the TOE by using the method described in [AGD_PRE], page 10 command in the device terminal.

The TOE has been configured as described in the [AGD_PRE], section “Security preparation of the Environment” and in document [IMC_INST_GUIDE], in section “Preparing for installation”.

EVALUATION RESULTS

The product iMC MagicBox (iMC PLAT, iMC EIA) version 7.3 (PLAT E0708P13, EIA E0629) has been evaluated against the Security Target *iMC MagicBox - Security Target, v3.4, 2025-07-08*.

All the assurance components required by the evaluation level EAL1 + ASE_SPD.1 have been assigned a “PASS” verdict. Consequently, the laboratory SGS Brightsight Barcelona, S.L. (Unipersonal) assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL1 + ASE_SPD.1, as defined by the Common Criteria v3.1 R5, the CEM v3.1 R5 and the collaborative Protection Profile for Network Devices, v.2.2e, 2020-03-23.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- Aside on strictly follow the secure configuration guidance in [AGD_OPE] and [AGD_PRE], no other recommendations were devised in this evaluation.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product iMC MagicBox (iMC PLAT, iMC EIA) version 7.3 (PLAT E0708P13, EIA E0629), a positive resolution is proposed.

GLOSSARY

AAA	Authentication, Authorization and Accounting
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IPSec	Internet >Protocol Security
OC	Organismo de Certificación
SSH	Secure Shell
TOE	Target Of Evaluation
TSFI	TOE Security Functional Interface

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[PP-ND] collaborative Protection Profile for Network Devices, v.2.2e, 2020-03-23.

[PP-ND-SUPPORT] CCDB-2019-12-004, Supporting Document Mandatory Technical Document, Evaluation Activities for Network Device cPP, December-2019, Version 2.2.

[AGD_PRE] Preparative and Operative Procedures for CC NDPP iMC Magicbox v1.4, 2024-09-18.

[AGD_OPE] [IMC_ADM_GUIDE], [IMC_INST_GUIDE], [IMC_USER_GUIDE], [IMC_UAM_CERT], [IMC_TAM_CERT], [IMC_PLAT_TRU], [IMC_UAM_TRU], [IMC_PLAT_CERT].

[IMC_ADM_GUIDE] H3C iMC Enterprise and Standard Platform Administrator Guide-7.3, 5W112.

[IMC_INST_GUIDE] H3C iMC MagicBox Installation Guide-7.3, 5W102.

[IMC_USER_GUIDE] H3C iMC User Access Manager Administrator Guide-7.3, 5W108.

[IMC_UAM_CERT] H3C iMC UAM Configuration Examples, 5PW103.

[IMC_TAM_CERT] H3C iMC TAM Configuration Examples, 5PW100.

[IMC_PLAT_TRU] H3C IMC PLAT Troubleshooting Guide, 5PW104.

[IMC_UAM_TRU] H3C iMC UAM Troubleshooting Guide, 5PW102.

[IMC_PLAT_CERT] H3C iMC PLAT Configuration Examples, 5W108.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- *iMC MagicBox - Security Target, v3.4, 2025-07-08*.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components selected.