Reference: 2022-32-INF-4559- v1
Target: Limitada al expediente
Date: 23.05.2025

Created by: CERT13
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2022-32**
TOE	**NetinDS v2.0.2**
Applicant	**B19310374 - Netin Systems S.L.**
References	

[EXT-7895] 2022-07-04_2022-32_solicitud_certificacion

[EXT-9313] Informe Técnico de Evaluación v1.0

Certification report of the product NetinDS v2.0.2, as requested in EXT-7895 dated 07/04/2022, and evaluated by jtsec Beyond IT Security, S.L., as detailed in the Evaluation Technical Report EXT-9313 received on 27/09/2024.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product NetinDS v2.0.2.

Netin Diagnostic System, better known as NetinDS, is a system for monitoring and diagnosing industrial installations and OT infrastructures, whose objective is to provide professionals with the necessary tools for the diagnosis of their installations. Designed and developed for the industry, NetinDS relies on the world's leading IT monitoring protocols as well as the most well-known and widespread OT standards. It is developed by Netin Systems SL. Integration with the IIoT platform (Industrial Internet of Things) in the way of digitalization is one of its main bases, and together with the integration with IT systems, it allows the creation of the necessary ecosystem to have the information available when and where it is needed. NetinDS helps with maintenance and operation tasks, making it possible to anticipate possible problematic situations and resolve them more efficiently.

Developer/manufacturer: Netin Systems S.L.

Sponsor: Netin Systems S.L..

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

ITSEF: jtsec Beyond IT Security.

Protection Profile: none.

Evaluation Level: Common Criteria version 3.1 release 5 EAL2.

Evaluation end date: 10/04/2025

Expiration Date[1]: 20/05/2030

All the assurance components required by the evaluation level EAL2 have been assigned a "PASS" verdict. Consequently, the laboratory jtsec Beyond IT Security, S.L. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2, as defined by the Common Criteria version 3.1 release 5 and the Common Criteria Evaluation Methodology version 3.1 release 5.

Considering the obtained evidences during the instruction of the certification request of the product NetinDS v2.0.2, a positive resolution is proposed.

[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.

TOE SUMMARY

NetinDS is a Network Management Software specially designed for monitoring industrial technology devices.

NetinDS is a distributed and agent-based system that monitors large OT infrastructures and modern industrial automation systems. The product doesn't provide a single deployment environment, since it allows a properly configuration accomplished with the specific operational environment and size of the organization. NetinDS, in its Standalone deployment mode, is the one covered from the scope of the Common Criteria Certification. In this version, NetinDS acts like agent and server as a single deployment.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2, according to Common Criteria v3.1 R5.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

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

- Cryptographic support:
  - FCS_CKM_EXT.2
  - FCS_CKM.1
  - FCS_CKM.2
  - FCS_COP.1/(4)
  - FCS_COP.1/(1)
  - FCS_COP.1/(3)
  - FCS_COP.1/(2)
  - FCS_RBG_EXT.1
  - FCS_RBG_EXT.2
  - FCS_CKM_EXT.1
  - FCS_STO_EXT.1
  - FCS_HTTPS_EXT.1
  - FCS_TLS_EXT.1
  - FCS_TLSS_EXT.1
- User data protection:
  - FDP_DEC_EXT.1
  - FDP_DAR_EXT.1
  - FDP_NET_EXT.1
- Security management:
  - FMT_SMF.1
  - FMT_MEC_EXT.1
  - FMT_CFG_EXT.1
- Trusted path/channels:
  - FTP_ITC.1/SNMPv3
  - FTP_DIT_EXT.1
- Privacy:

- FPR_ANO_EXT.1

- Protection of the TSF:
  - FPT_API_EXT.1
  - FPT_AEX_EXT.1
  - FPT_IDV_EXT.1
  - FPT_TUD_EXT.1
  - FPT_TUD_EXT.2

IDENTIFICATION

Product: NetinDS v2.0.2

Security Target: NetinDS Security Target v0.15

Protection Profile: none.

Evaluation Level: Common Criteria version 3.1 release 5 EAL2.

SECURITY POLICIES

Organizational Security Policies (OSP) are not defined in the Security Target.

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 3.4 Assumptions.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product NetinDS v2.0.2, although the agents implementing attacks have the attack potential according to the Basic of EAL2 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 3.3 Threats to Security.

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

The TOE includes several security features. Each of the security features identified above consists of several security functionalities and are considered TOE Security Functionalities, as identified below.

- Cryptographic support. The objective is to help to satisfy several high-level security objectives. These include secure storage of passwords, and data integrity, trusted channel. This is done in order to establish secure channels for remote TOE's administration and communication between the TOE and external IT entities.
- Security Management. Specifies the management of several aspects of the TSF: security attributes and TSF data and functions. Via the web interface, it is possible for administrators the management of the agent, artifacts, users, configuration and maintenance.
- Trusted path. Provides protection of all the communications between the TOE and users and administrators and external IT entities. Trusted channels are provided by SNMPv3 and TLSv1.2. In parallel, TLS provides support for MQTTv3.1.1 and HTTPS protocols.
- User data protection and privacy. The TOE limits its access to necessary hardware resources and information repositories. Data at non-volatile memory is encrypted. The TOE does not share PII with third parties.
- Protection of the TSF. The application has been developed with attack prevention mechanisms in accordance to high quality standards. The TOE incorporates memory anti-exploitation capabilities. The TOE is versioned, signed and distributed as additional software. APIs used by the TOE are documented.

PHYSICAL ARCHITECTURE

The Target of Evaluation (TOE) is purely a software TOE and includes the following components:

Delivery Item	Type	Version	Delivery Method	Format
netin-ds-agent-installer-1.0.0	Software	2.0.2	Download from an FTP server with TLS encryption	.exe
Operational User Guidance	Guidance Documentation	0.12	Download from an FTP server with TLS encryption	PDF
Preparative Procedures	Preparative Documentation	0.12	Download from an FTP server with TLS encryption	PDF
Netin Documentation	User Documentation	0.1	Download from an FTP server with TLS encryption	PDF

DOCUMENTS

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

- NetinDS Preparative Procedures v0.12 [AGD_PRE]
- NetinDS Operational User Guidance v0.12 [AGD_OPE]
- Netin Documentation v0.1 [NETIN_DOC]
- NetinDS Security Target v0.15 [ST]

PRODUCT TESTING

The independent testing approach has been testing all the SFRs declared in the Security Target, all the TSFIs declared in the Functional Specification and all the subsystems declared in the TOE Design.

Regarding the repetition of the developer's functional tests, all of the tests defined in the test plan provided by the manufacturer have been repeated to verify their results obtained.

On the other hand, the vulnerability analysis approach has been based in:

- Search of public vulnerabilities for the TOE components and the third-party libraries used by the TOE.
- Identification of possible vulnerabilities in the Security Target, Guidance documentation, Functional Specification, TOE Design and Security Architecture evidences.

Based on the vulnerabilities found, the evaluator calculated the attack potential and designed a test for each vulnerability with Basic attack potential.

EVALUATED CONFIGURATION

NetinDS supports three different installations: NetinDS Standalone, NetinDS Server and NetinDS mix. Only NetinDS Standalone mode is covered by the scope of this evaluation. NetinDS Standalone installation mode acts in a single deployment as server and agent, installed in a single computer, while in other NetinDS operational modes, server and agent are in different distributed deployments. The TOE evaluated configuration can be described as follows:

The external IT entities associated with NetinDS are integrated by the administrators through management operations. These external IT entities will be monitored using a secure channel through SNMPv3/MQTTv3.1.1 protocol connected to NetinDS Agent. Data generated by external IT entities will be sent from NetinDS Agent to NetinDS Server to be monitored by the administrators and users. The TOE has to be configured to use HTTPS in the secure communication channel between remote administrators and Nginx. The evaluated configuration requires the TOE operational environment to be equipped with the NON-TOE HW/FW/SW described in section 1.3.4 of the Security Target. In order to achieve the above-described configuration, the TOE preparative guides ([AGD_PRE]) must be thoroughly followed for the TOE installation and configuration.

A minimum deployment required to obtain functional system would be as follow:

NetinDS Standalone mode (Server and Agent included).

A number of external IT entities connected to the NetinDS through a proper protocol (only SNMPv3 and MQTTv3.1.1 are allowed under the scope of certification).

Apart from these considerations, the TOE does not require any other pre-configuration or particular usage to obtain the security features described in this document beyond the TOE guide's steps.

EVALUATION RESULTS

The product NetinDS v2.0.2 has been evaluated against the Security Target NetinDS Security Target v0.15.

All the assurance components required by the evaluation level EAL2 have been assigned a "PASS" verdict. Consequently, the laboratory jtsec Beyond IT Security, S.L. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2, as defined by the Common Criteria version 3.1 release 5 and the Common Criteria Evaluation Methodology version 3.1 release 5.

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.

The MQTT broker from the TOE does not require credentials to establish connections. Given this, if the TOE is misconfigured and a MQTT template is associated with a potential attacker device, such device is able to connect. It is recommended to carry out an inventory of the network devices monitored by the TOE so unknown devices can be detected.

Some of the third-party components of the TOE have public CVEs assigned, although they were not proved exploitable given the functionality of the TOE and the defined security problem, it is recommendable to update them.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product NetinDS v2.0.2, a positive resolution is proposed.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

OC Organismo de Certificación

TOE Target Of Evaluation

BIBLIOGRAPHY

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

[CC31R5P1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 Final, April 2017.

[CC31R5P2] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 Final, April 2017.

[CC31R5P3] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 Final, April 2017.

[CEM31R5P3] Common Criteria Evaluation methodology, Version 3.1, Revision 5 Final, April 2017.

[SOG-IS] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms. Version 1.2. January 2020

[STIC-807] Guía de Seguridad de las TIC CCN-STIC 807. Criptología de empleo en el Esquema Nacional de Seguridad. May 2022

[AGD_PRE] NetinDS Preparative Procedures v0.12

[AGD_OPE] NetinDS Operational User Guidance v0.12

[NETIN_DOC] Netin Documentation v0.1

[ST] NetinDS Security Target v0.15

SECURITY TARGET

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

- NetinDS Security Target v0.15.

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.