Reference: 2024-5-INF-4717- v1	Created by: I008
Target: Limitada al expediente	Revised by: CALIDAD
Date: 23.02.2026	Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2024-5**
TOE	**ESET Endpoint Security v12.1.2057.3**
Applicant	**SK2020317068 - ESET spol. s r.o.**

References

[EXT-8995] Solicitud certificación

[EXT-9941] 2025-12-18_2024-05_ETR_v1.1

Certification report of the product ESET Endpoint Security v12.1.2057.3, as requested in [EXT-8995] dated 08/04/2024, and evaluated by jtsec Beyond IT Security, S.L., as detailed in the Evaluation Technical Report [EXT-9941] received on 18/12/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product ESET Endpoint Security v12.1.2057.3.

ESET Endpoint Security, is an endpoint protection solution that provides a variety of security features to protect their systems from a wide range of threats. ESET Endpoint Security is primarily designed for use on workstations in a business environment.

Developer/manufacturer: ESET spol. s r.o.

Sponsor: ESET spol. s r.o..

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

ITSEF: JTSEC.

Protection Profile: NIAP Protection Profile for Application Software version 1.4, dated 10 October 2021. [PPAPP14]

Evaluation level: Common Criteria Version 3.1 Release 5 (assurance packages according to [PPAPP14]).

Evaluation end date: 23/12/2025

Expiration Date[1]: 24/02/2031

All the assurance components required by the evaluation level of [PPAPP14] 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 [PPAPP14] assurance level packages, as defined by the Common Criteria Version 3.1 Release 5, April 2017, [PPAPP14] 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 ESET Endpoint Security v12.1.2057.3, 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

The TOE is an application software which runs on a Windows platform that provides malware detection and mitigation in the system where it is installed.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the assurance packages defined in [PPAPP14], according to Common Criteria v3.1 R5. The TOE meets the following SARs:

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.2
	ASE_REQ.2
	ASE_TSS.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 and [PPAPP14]:

- Cryptographic Support
  - FCS_CKM_EXT.1
  - FCS_RBG_EXT.1
  - FCS_STO_EXT.1
- User Data Protection
  - FDP_DEC_EXT.1
  - FDP_NET_EXT.1

  - FDP_DAR_EXT.1
- Security Management
  - FMT_MEC_EXT.1
  - FMT_CFG_EXT.1
  - FMT_SMF.1
- Privacy
  - FPR_ANO_EXT.1
- Protection of the TSF
  - FPT_API_EXT.1
  - FPT_AEX_EXT.1
  - FPT_IDV_EXT.1
  - FPT_LIB_EXT.1
  - FPT_TUD_EXT.1
  - FPT_TUD_EXT.2
- Trusted Path/Channels
  - FTP_DIT_EXT.1
- Identification and Authentication
  - FIA_X509_EXT.1
  - FIA_X509_EXT.2

IDENTIFICATION

Product: ESET Endpoint Security v12.1.2057.3

Security Target: ESET Endpoint Security - Security Target Version: 0.2

Protection Profile: NIAP Protection Profile for Application Software version 1.4, dated 10 October 2021.

Evaluation Level: Common Criteria Version 3.1 Release 5 (assurance packages according to [PPAPP14]).

SECURITY POLICIES

The use of the product ESET Endpoint Security v12.1.2057.3 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

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 3.2 Assumptions.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product ESET Endpoint Security v12.1.2057.3, although the agents implementing attacks have the attack potential according to the Basic 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 3.1 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 [PP] 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
- User Data Protection
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channel
- Identification and Authentication

PHYSICAL ARCHITECTURE

The TOE is a software-only application running standalone on a Windows operating system platform, such platform is not considered part of the TOE.

- Format: msi format.
- File name: ees_nt64.msi
- Delivery Method: Downloadable from official ESET website.
- TOE version: 12.1.2057.3
- SHA256 hash: EC602625147A2B4B6845201D6632CB6F1D8F5C3753EE8696A96B1736D026B7A8

The following table lists the documents and user's guide necessary to carry out the configuration of the TOE properly:

Item	Description	Version / Hash	Delivery Method	Format
ESET Endpoint Security Preparational Guidance for Common Criteria	Documents for the safe acceptance of the TOE and the installation and configuration process	0.3	Email on customer request	PDF
ESET Endpoint Security	Documents describing	0.2	Email on customer request	PDF

Operational Guidance for Common Criteria	the safe use of the TOE.			
ESET Endpoint Security User Guide (eset_endpoint_security_12_enu.pdf)	Official guide available in ESET website.	REV. 10/1/2025 SHA 256 BC3A51157C0B271E000AFAC5CB9C46AE9257766E2B1CA77CBD0F76E43E42E51B	Online help portal: https://help.eset.com/ees/12/en-US/	Online PDF available for download

DOCUMENTS

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

- Preparational Guidance for Common Criteria v0.3: documents for the safe acceptance of the TOE and the installation and configuration process.
- Operational Guidance for Common Criteria v0.2: Documents describing the safe use of the TOE.
- ESET Endpoint Security User Guide REV 10/1/2025: Official ESET Endpoint Security user guidance.

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.

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.

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

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product ESET Endpoint Security v12.1.2057.3 it is necessary the disposition of the following software components:

- Selected TOE capabilities on installation:
  - Protections:
    - Real-time file system protection
    - Network access protection
    - Device control
    - Document protection
  - Computer scan
- Post installation tasks:
  - Configuring HTTPS profile for updates
  - Advanced setup and uninstall protection
  - Restricting TLS configuration (TLS versions and TLS cipher suites)

EVALUATION RESULTS

The product ESET Endpoint Security v12.1.2057.3 has been evaluated against the Security Target ESET Endpoint Security - Security Target Version: 0.2.

All the assurance components required by the evaluation level [PPAPP14] 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 assurance packages defined according to the Common Criteria Version 3.1 Release 5, April 2017, the [PPAPP14] and the Common Criteria Evaluation methodology, Version 3.1, Release 5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

No recommendations were generated for this evaluation.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product ESET Endpoint Security v12.1.2057.3, 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:

[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.

[PPAPP14] Protection Profile for Application Software, Version 1.4, 2021-10-07

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.