Reference: 2020-67-INF-4627- v1
Target: Limitada al expediente
Date: 02.09.2025

Created by: CERT15
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2020-67**
TOE	**Endpoint Security Host Agent vE88.50 (88.50.0220)**
Applicant	**520042821 - Check Point Software Technologies Ltd.**

References

[EXT-6466] 2020-12-01_2020-67_solicitud_certificacion

[EXT-9232] 2024-09-06_2020-67_ETR_v2

Certification report of the product Endpoint Security Host Agent vE88.50 (88.50.0220), as requested in [EXT-6466] dated 01/12/2020, and evaluated by jtsec Beyond IT Security, S.L., as detailed in the Evaluation Technical Report [EXT-9232] received on 06/09/2024.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Endpoint Security Host Agent vE88.50 (88.50.0220).

Endpoint Security Host Agent, better known as Endpoint Security, is an antivirus software to monitor and secure computers deployed in corporate networks. It is part of a Cloud solution where the TOE is the agent and the Harmony Endpoint EPMaaS is the cloud component in charge of management of the agents.

Developer/manufacturer: Check Point Software Technologies Ltd.

Sponsor: Check Point Software Technologies Ltd..

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

ITSEF: jtsec Beyond IT Security, S.L..

Protection Profile:

The Security Target claims exact conformance with the following protection profile:

- NIAP Protection Profile for Application Software version 1.4, dated 07 October 2021 with exact conformance.

The Security Target claims conformance with the following package:

- NIAP Functional Package for TLS Version 1.1, dated 12 February 2019.

Evaluation Level: Common Criteria version 3.1 release 5 (assurance packages according to [NIAPPPAS], [NIAPFPTLS])

Evaluation end date: 28/07/2025

Expiration Date[1]: 22/08/2030

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

[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.

Considering the obtained evidences during the instruction of the certification request of the product Endpoint Security Host Agent vE88.50 (88.50.0220), a positive resolution is proposed.

TOE SUMMARY

The TOE is an antivirus software which is part of a client-server architecture intended to be used on computers deployed in a corporate network. These computers will be connected to each other and will carry out information processing to a central server that manages this information in a server-centric architecture. This central server, called Harmony Endpoint EPMaaS is in the cloud and is accessed from the Check Point Infinity Portal.

The TOE is intended to be installed in each computer of the network's organization. Once installed, the TOE carries out the communication to the Harmony Endpoint EPMaaS and monitors the security status of the computer where it has been installed and also synchronises this status with the server. Simultaneously, during this synchronisation process, the TOE applies the Harmony Endpoint EPMaaS's security policies.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the assurance packages defined in [NIAPPPAS], according to Common Criteria version 3.1 release 5. 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.1
	ASE_REQ.1
	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:

- Cryptographic support
    - FCS_CKM.2
    - FCS_CKM.1/AK
    - FCS_CKM.1/SK
    - FCS_CKM_EXT.1/PBKDF
    - FCS_COP.1/SKC
    - FCS_COP.1/Hash
    - FCS_COP.1/Sig
    - FCS_COP.1/KeyedHash
    - FCS_RBG_EXT.1
    - FCS_RBG_EXT.2
    - FCS_CKM_EXT.1
    - FCS_STO_EXT.1
    - FCS_HTTPS_EXT.1/Client HTTPS Protocol
    - FCS_TLS_EXT.1
    - FCS_TLSC_EXT.1
- Security management:
    - FMT_SMF.1
    - FMT_MEC_EXT.1
    - FMT_CFG_EXT.1
- User data protection
    - FDP_DEC_EXT.1
    - FDP_NET_EXT.1
    - FDP_DAR_EXT.1
- Privacy
    - FPR_ANO_EXT.1
- Protection of the TSF

- FPT_API_EXT.1
- FPT_AEX_EXT.1
- FPT_TUD_EXT.1
- FPT_TUD_EXT.2
- FPT_LIB_EXT.1
- FPT_IDV_EXT.1

- Trusted path/channels
  - FTP_DIT_EXT.1
- Identification and authentication
  - FIA_X509_EXT.1
  - FIA_X509_EXT.2

IDENTIFICATION

Product: Endpoint Security Host Agent vE88.50 (88.50.0220)

Security Target: Check Point Endpoint Security Host Agent - Security Target v1.9

Protection Profile:

The Security Target claims exact conformance with the following protection profile:

- NIAP Protection Profile for Application Software version 1.4, dated 07 October 2021 with exact conformance.

The Security Target claims conformance with the following package:

- NIAP Functional Package for TLS Version 1.1, dated 12 February 2019.

Evaluation Level: Common Criteria version 3.1 release 5 (assurance packages according to [NIAPPPAS], [NIAPFPTLS])

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 3.2 Assumptions.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Endpoint Security Host Agent vE88.50 (88.50.0220), 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 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 and Data Protection
- Security Management
- Identification and Authentication
- Protection of the TSF

- Trusted Path/Channels

PHYSICAL ARCHITECTURE

The TOE is a software-only evaluation running on a Windows OS platform. The following minimum requirements are needed for the underlying platform to ensure the TOE functions as required:

Operating System: Windows 10 or later.

- RAM: 2GB.
- Hard Drive: 2GB
- Format: exe format.
- File name: EPS__V88.50.0220.exe
- Delivery Method: official website.
- TOE version: vE88.50 (88.50.0220)

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

Document	Version	Format	Delivery Method
Infinity portal Administration Guide	10 July 2024	PDF document	Email on customer request
Harmony Endpoint EPMAAS Administration Guide	09 July 2024	PDF document	Email on customer request
Endpoint Security Clients For Windows User Guide	02 May 2024	PDF document	Email on customer request

DOCUMENTS

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

- Infinity portal Administration Guide, 10 July 2024 [INFINITY_DOC]
- Harmony Endpoint EPMAAS Administration Guide, 9 July 2024 [HARMONY_DOC]

- Endpoint Security Clients For Windows User Guide, 02 May 2024 [ENDPOINT_DOC]
- Check Point "Harmony" Endpoint Security Host Agent - Security Target v1.9 [ST]
- Check Point Endpoint Security Host Agent - Operational User Guidance v0.7 [AGE_OPE]
- Check Point Endpoint Security Host Agent – Preparative procedures v0.6 [AGD_PRE]

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 TOE evaluated version is Check Point Endpoint Security Host Agent vE88.50 (88.50.0220), and has been configured according to [AGD_PRE], the evaluated configuration is:

- Selected TOE capabilities:
  - Anti Malware
  - Anti Bot and URL Filtering
  - Anti Ransomware, Behavioral Guard and Forensics
  - Threat Emulation and Anti Exploit
  - Compliance
- Installed with the following command to force TLSv1.2 communication channels:
  - *EPS.msi FORCETLS12=1*

For the Operational environment it is necessary to disable TLS cipher suites based on 3DES.

EVALUATION RESULTS

The product Endpoint Security Host Agent vE88.50 (88.50.0220) has been evaluated against the Security Target Check Point "Harmony" Endpoint Security Host Agent - Security Target v1.9.

All the assurance components defined in the [NIAPPPAS] and [NIAPFPTLS] 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 assurances packages defined, according to the Common Criteria v3.1 release 5, the [NIAPPPAS] and [NIAPFPTLS] and the CEM v3.1 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.

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 Endpoint Security Host Agent vE88.50 (88.50.0220), 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
ST	Security Target
OE	Operational Environment

Augmentation

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.

[NIAPPPAS] NIAP Protection Profile for Application Software version 1.4, dated 07 October 2021.

[NIAPFPTLS] NIAP Functional Package for TLS Version 1.1, dated 12 February 2019

[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

[INFINITY_DOC] Infinity portal Administration Guide, 10 July 2024

[HARMONY_DOC] Infinity portal Administration Guide, 10 July 2024

[ENDPOINT_DOC] Endpoint Security Clients For Windows User Guide, 02 May 2024

[ST] Check Point “Harmony” Endpoint Security Host Agent - Security Target v1.9

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

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

- Check Point “Harmony” Endpoint Security Host Agent - Security Target v1.9

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 assurance components up to EAL4.

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.