PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2024/07

HarfangLab EDR

Version 3.0.4

Paris, le 22 Août 2024

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2024/07

Nom du produit

HarfangLab EDR

Référence/version du produit

Version 3.0.4

Catégorie de produit

Détection d'intrusions

Critère d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)

Commanditaire

HARFANGLAB
Campus Cyber – Tour ERIA – 5-7 rue Bellini
92800 Puteaux, France

Développeur

HARFANGLAB
Campus Cyber – Tour ERIA – 5-7 rue Bellini
92800 Puteaux, France

Centre d'évaluation

THALES / CNES
290, allée du Lac
31670 Labège, France

Accord de reconnaissance applicable

fixed time certification

Ce certificat est reconnu dans le cadre du [BSZ_CSPN]

Fonctions de sécurité évaluées

Authentification entre agent et manager
Identification des agents
Vérification de mise à jour d'agent
Confidentialité et intégrité du trafic utilisateur
Cloisonnement de l'exécution sur agent
Protection de l'exécution sur agent
Stockage des données en déconnecté
Limitation des droits utilisateurs sur le manager
Limitation des droits et isolation des composants manager
Vérification des données entrantes
Contrôle d'accès manager

Sécurisation des interconnexions
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Oui (cf. §3.2)

PREFACE

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit 7
1.1 Présentation du produit 7
1.2 Description du produit évalué 8
1.2.1 Catégorie du produit 8
1.2.2 Identification du produit 8
1.2.3 Fonctions de sécurité 9
1.2.4 Configuration évaluée 9
2 L'évaluation 10
2.1 Référentiels d'évaluation 10
2.2 Travaux d'évaluation 10
2.2.1 Installation du produit 10
2.2.2 Analyse de la documentation 10
2.2.3 Revue du code source (facultative) 10
2.2.4 Analyse de la conformité des fonctions de sécurité 10
2.2.5 Analyse de la résistance des mécanismes des fonctions de sécurité 10
2.2.6 Analyse des vulnérabilités (conception, construction, etc.) 11
2.2.7 Analyse de la facilité d'emploi 11
2.3 Analyse de la résistance des mécanismes cryptographiques 12
2.4 Analyse du générateur d'aléa 12
3 La certification 13
3.1 Conclusion 13
3.2 Recommandations et restrictions d'usage 13
3.3 Reconnaissance du certificat 13
ANNEXE A. Références documentaires du produit évalué 14
ANNEXE B. Références liées à la certification 15

1 Le produit

1.1 Présentation du produit

Le produit évalué est « HarfangLab EDR, Version 3.0.4 » développé par HARFANGLAB.

Le produit HarfangLab EDR (*Endpoint Detection and Response*) est un système logiciel de détection, d'investigation et de réponse aux incidents de sécurité susceptibles d'affecter les postes de travail et les serveurs informatiques (*endpoints*).

Il se compose de sondes de postes, ou agents logiciels installés sur les postes à surveiller, et d'un manager centralisé qui traite et conserve des données de télémétrie ainsi que les évènements et les alertes.

Les agents embarquent des fonctionnalités de détection et de remédiation, ils transmettent des données au manager automatiquement (télémétrie) ou via des jobs d'investigation.

Le manager de l'EDR se compose de plusieurs modules fonctionnels *(Collect, Analytics, View, Connect)* qui permettent notamment de piloter et d'administrer la solution et les agents.

La figure ci-dessous explicite l'architecture du produit.

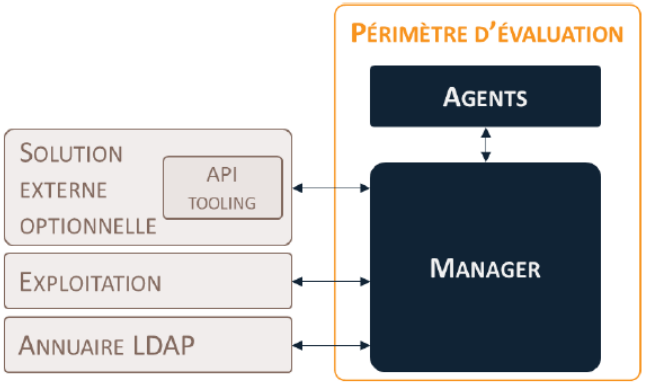


Figure 1 - Architecture Produit.

Le présent certificat porte sur les agents et le manager, avec notamment :

- la protection du manager vis-à-vis des entités externes avec lesquelles il interagit (agents, utilisateurs et services externes) ;
- la protection des données échangées entre le manager et les services externes ;
- l'innocuité de l'agent (pas de dégradation des machines sur lesquelles l'agent est déployé) ;
- l'autoprotection de l'agent (pas de désactivation du service EDR ou de désinstallation de l'agent par un utilisateur).

Le certificat ne couvre pas les fonctions suivantes, qui sont hors du périmètre d'évaluation :

- pour le manager : les fonctions d'analyse de données ;
- pour les agents : la surveillance des processus, le relevé d'informations.

1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 *Catégorie du produit*

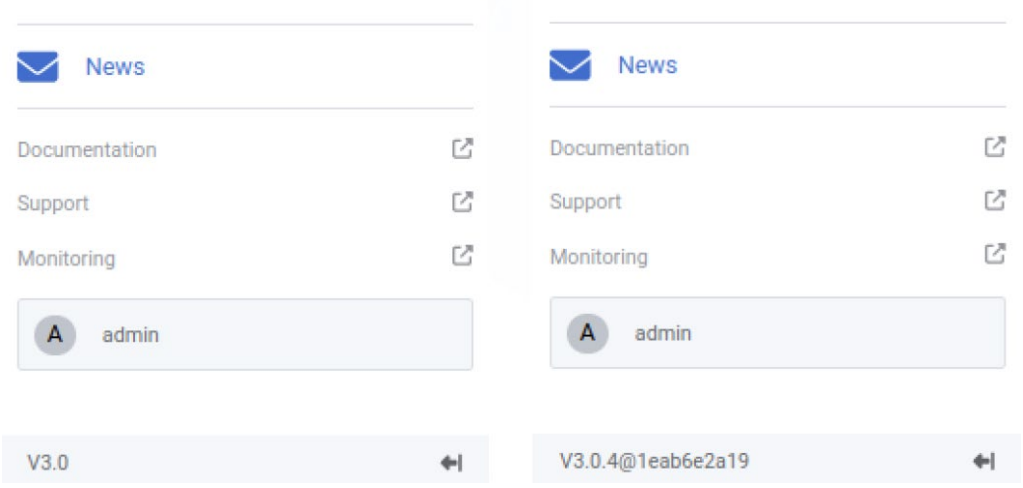
☒	**1**	**détection d'intrusions**
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☐	6	identification, authentification et contrôle d'accès
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☐	9	stockage sécurisé
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

1.2.2 *Identification du produit*

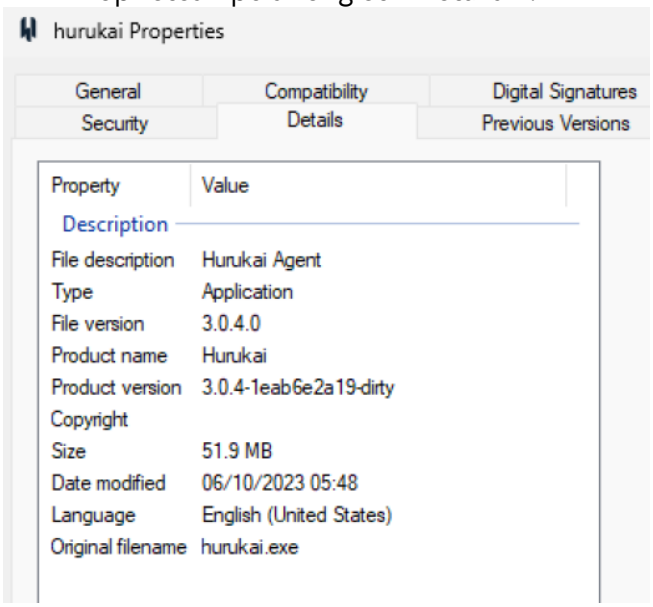
Produit	
Nom du produit	HarfangLab EDR
Numéro de la version évaluée	Version 3.0.4

La version certifiée du produit peut être identifiée de la manière suivante :

- pour le manager :
  - dans l'interface d'administration, double cliquer sur le numéro de version qui apparait en bas à gauche de l'interface, afin d'afficher la version complète :



- Pour l'agent :
  - faire un clic droit sur l'exécutable « `hurukai.exe` » situé dans le répertoire d'installation de l'agent `C:\Program Files\HarfangLab`, puis sélectionner « Propriétés » puis l'onglet « Détails » :



1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'authentification entre agent et manager ;
- l'identification des agents ;
- la vérification de mise à jour d'agent ;
- la confidentialité et l'intégrité du trafic utilisateur ;
- le cloisonnement de l'exécution sur agent ;
- la protection de l'exécution sur agent ;
- le stockage des données en déconnecté ;
- la limitation des droits utilisateurs sur le manager ;
- la limitation des droits et isolation des composants manager ;
- la vérification des données entrantes ;
- la contrôle d'accès manager ;
- la sécurisation des interconnexions.

1.2.4 *Configuration évaluée*

La plateforme d'évaluation du produit est constituée d'une configuration standard de manager sous la forme d'une machine virtuelle et de l'agent sur une version de référence de Windows :

- pour l'agent, dernière version de Windows 11 disponible au début des tests ;
- pour le manager, dernière version de Windows *Server* 2022 disponible au début des tests.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

2.2 Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

2.2.1.2 Description de l'installation et des non-conformités éventuelles

L'installation est relativement complexe et doit être réalisée par le développeur ou avec son assistance.

Le manager est installé en premier, suivi de l'installation du ou des agents.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 *Analyse de la documentation*

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.2.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS].

2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS].

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 Cas où la sécurité est remise en cause

Les risques identifiés lors de l'évaluation entraînent des recommandations [ET/OU] des restrictions d'usage pour l'utilisateur (voir chapitre 3.2).

2.2.7.2 Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.2.7.3 Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé. Afin que les mécanismes analysés soient conformes aux exigences de ce référentiel, les recommandations identifiées [GUIDES] doivent être suivies.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « HarfangLab EDR, Version 3.0.4 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- l'installation du produit certifié doit être réalisée par le développeur ou avec son assistance ;
- le mécanisme de protection « Self-protection » de l'agent doit être activé.

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions de l'accord du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ *(Beschleunigte Sicherheitszertifizierung* ou Certification de sécurité accélérée).

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - *EDR HarfangLab Endpoint Detection & Response* – Cible de sécurité, référence DINT-KLIF-CIBLE-01 Ed 7, version 7.0, 24 juin 2024.
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN *FUMSECK*, référence FUMSECK_CSPN-RTE_FR, version 1.4, 15 juillet 2024.
[GUIDES]	Guide d'utilisation, d'administration et d'installation du produit : - Documentation d'installation EDR HarfangLab, référence DTU-2-01-INSTALL, version 2.1, 21 mars 2024 ; - Manuel utilisateur EDR HarfangLab, référence DTU-2-02-USER, version 1.4, 21 mars 2024 ; - Manuel d'administration EDR HarfangLab, référence DTU-ADMIN-03, version 1.5, 21 mars 2024 ; - HarfangLab EDR Documentation, version 3.0, 21 mars 2024.

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01, version 5.0, 12 janvier 2023. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0,6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[BSZ_CSPN]	*Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence *bsz_cspn_mutual_recognition_agreement,*version 2.0, mai 2024.