PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2020/43

Agent EDR

Hurukai v2.0.1

Paris le 24 décembre 2020

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

Guillaume POUPARD

[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-2020/43**
Nom du produit **Agent EDR**
Référence/version du produit **Hurukai v2.0.1**
Catégorie de produit **Détection d'intrusions**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **HarfangLab** 55 rue de la Boétie 75008 PARIS
Développeur **HarfangLab** 55 rue de la Boétie 75008 PARIS
Centre d'évaluation **THALES / CNES** 290, allée du Lac 31670 Labège, France
Fonctions de sécurité évaluées Gestion de l'authentification Protection en confidentialité et intégrité du trafic utilisateur Cloisonnement de l'exécution Protection de l'exécution
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Oui (voir §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 www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit 6
1.1 Présentation du produit 6
1.2 Description du produit évalué 6
1.2.1 Catégorie du produit 7
1.2.2 Identification du produit 7
1.2.3 Fonctions de sécurité 8
1.2.4 Configuration évaluée 8
2 L'évaluation 9
2.1 Référentiels d'évaluation 9
2.2 Charge de travail prévue et durée de l'évaluation 9
2.3 Travaux d'évaluation 9
2.3.1 Installation du produit 9
2.3.2 Analyse de la documentation 9
2.3.3 Revue du code source (facultative) 9
2.3.4 Analyse de la conformité des fonctions de sécurité 10
2.3.5 Analyse de la résistance des mécanismes des fonctions de sécurité 10
2.3.6 Analyse des vulnérabilités (conception, construction, etc.) 10
2.3.7 Accès aux développeurs 10
2.3.8 Analyse de la facilité d'emploi 10
2.4 Analyse de la résistance des mécanismes cryptographiques 10
2.5 Analyse du générateur d'aléas 11
3 La certification 12
3.1 Conclusion 12
3.2 Recommandations et restrictions d'usage 12
ANNEXE A. Références documentaires du produit évalué 13
ANNEXE B. Références à la certification 14

1 Le produit

1.1 Présentation du produit

Le présent certificat porte sur l'« Agent EDR, Hurukai v2.0.1 » développé par HarfangLab.

Cet agent est un des éléments de la solution EDR (« *Endpoint Detection & Response* ») de l'éditeur HarfangLab. L'objectif de cette solution est de fournir une interface centrale permettant de détecter, investiguer et neutraliser les activités malveillantes sur un système d'informations. Les agents sont déployés par un administrateur du SI sur les postes soumis à surveillance (ou *Endpoints*), à raison d'un agent par poste. L'ensemble des agents sont gérés par un *Manager EDR* distant, qui récolte les informations extraites et les centralise afin qu'elles puissent par la suite être exploitées lors des différentes tâches de surveillance, détection et investigation.

La figure suivante donne une vision d'ensemble de l'environnement de l'EDR :

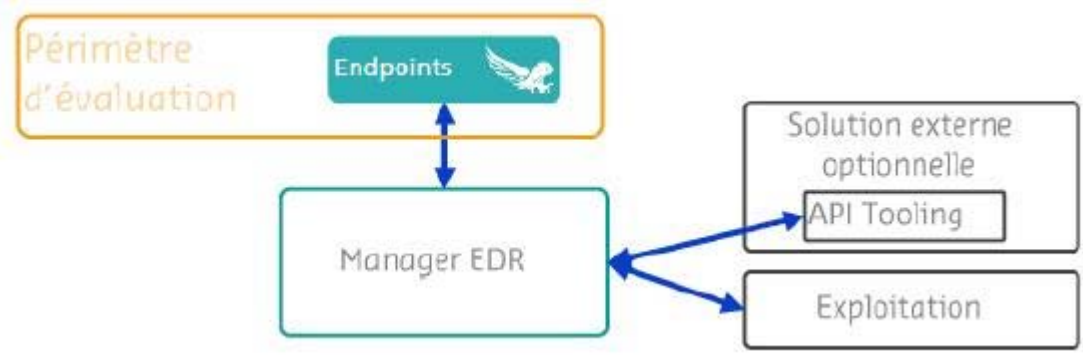

Figure 1 – Environnement de la TOE.

La figure ci-dessous présente l'architecture de l'agent déployé sur un poste. Il est constitué d'un service EDR et d'un module noyau, tous deux soumis à évaluation :

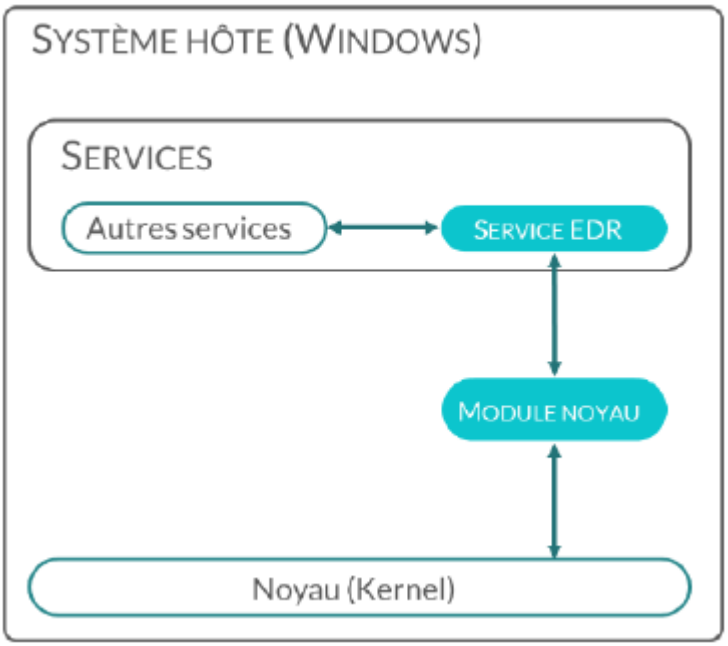

Figure 2 – Architecture de l'agent sur le poste.

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	Agent EDR
Numéro de la version évaluée	Hurukai v2.0.1

Les propriétés de l'exécutable « hurukai.exe » permettent d'identifier la version du produit évalué :

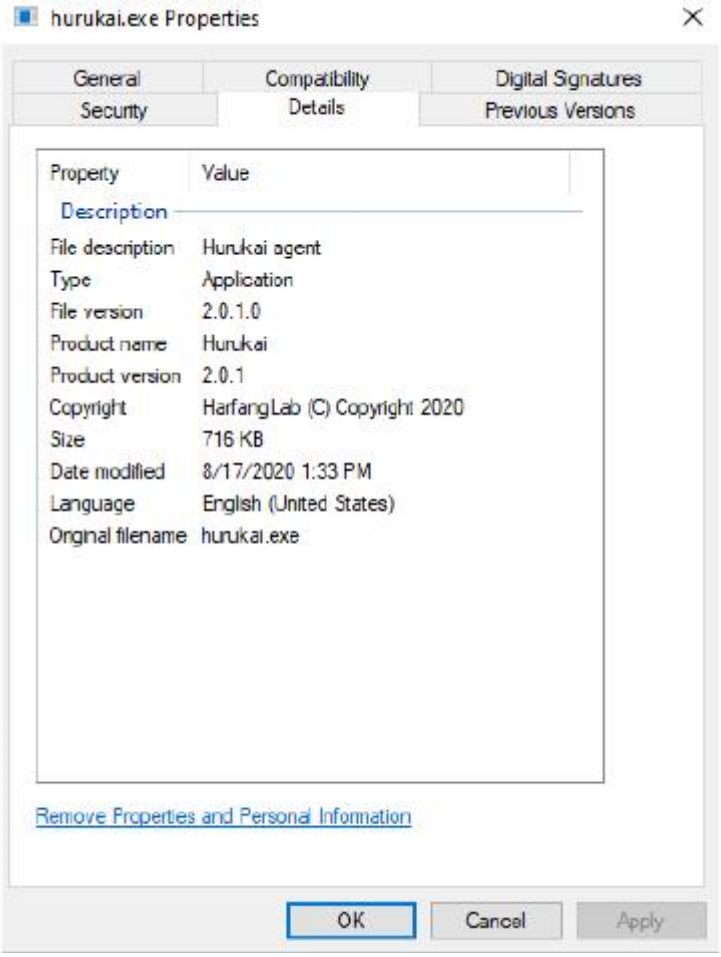

Figure 3 : affichage de la version du produit

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- la gestion de l'authentification ;
- la protection en confidentialité et intégrité du trafic utilisateur ;
- le cloisonnement de l'exécution ;
- la protection de l'exécution.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond au binaire « de production » du produit évalué.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

2.2 Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3 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].

2.3.1 *Installation du produit*

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

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

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

L'environnement mis en place pour l'évaluation est composé des éléments suivants déployés sur un réseau commun :

- une machine virtuelle Debian prête à l'emploi contenant un *manager* installé et en fonctionnement. La mise en place du *manager* n'est pas dans le périmètre de l'évaluation.
- une machine virtuelle Windows 10 conforme aux hypothèses de la cible de sécurité sur laquelle la TOE a été installée.

La section « 3) Déploiement des agents » du document d'installation (voir [GUIDES]) contient la démarche à suivre pour déployer les agents. Deux méthodes sont possibles : installation graphique et non graphique. Les deux méthodes ont été testées pendant l'évaluation.

2.3.1.3 Durée de l'installation

Moins de 10 minutes.

2.3.1.4 Notes et remarques diverses

Sans objet.

2.3.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

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

2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'intégralité du produit. L'analyse a été effectuée à l'aide de l'outil CppCheck.

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

2.3.4 *Analyse de la conformité des fonctions de sécurité*

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

2.3.5 *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.

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

2.3.6.1 Liste des vulnérabilités connues

Aucune vulnérabilité publique n'a été relevée concernant le produit ou ses briques logicielles tierces.

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS] et les restrictions d'usage définies dans la section 3.2.

2.3.7 *Accès aux développeurs*

Sans objet.

2.3.8 *Analyse de la facilité d'emploi*

2.3.8.1 Cas où la sécurité est remise en cause

Sans objet.

2.3.8.2 Avis d'expert sur la facilité d'emploi

L'évaluateur signale qu'aucune fonctionnalité pouvant accidentellement dégrader la sécurité de l'agent (mauvaise configuration, inattention) n'a été identifiée pendant l'évaluation.

Bien que le *manager* ne soit pas dans le périmètre de l'évaluation, l'évaluateur signale également que son interface est facile à prendre en main et que les informations sont présentées de manière claire et intuitive avec un vocabulaire adapté.

2.3.8.3 Notes et remarques diverses

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

2.4 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de vulnérabilité exploitable.

2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé. Si sa conception n'a pas mis en lumière de vulnérabilité, il s'appuie néanmoins sur la fonction *CryptGenRandom()* du système d'exploitation sous-jacent (Windows). La documentation de cette fonction n'est pas complète et son code source n'est pas disponible – il n'est donc pas possible d'en faire une analyse complète au sens de la méthodologie CSPN.

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 « Agent EDR, version Hurukai v2.0.1 » 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 mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations et restrictions suivantes :

- il est impératif pour les administrateurs de la solution d'effectuer des vérifications régulières de l'état de chargement des *drivers* via l'interface Kibana, ainsi que le préconise le guide d'administration dans sa section 6 (voir [GUIDES]). En pratique, les évènements suivants peuvent signaler une attaque par désinstallation de l'agent ou du *driver*, et doivent donc systématiquement être investigués par l'administrateur de l'EDR :
    - *driver is missing from our package directory ;*
    - *driver config is present in registry but not on disk;*
    - *driver enabled in config, installed, but failed to connect*
- les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les recommandations du document d'installation (voir [GUIDES]) doivent être appliquées ;
- les utilisateurs doivent impérativement se conformer aux recommandation du guide d'utilisation [GUIDES].

ANNEXE A. Références documentaires du produit évalué

[CDS]	*Endpoint Detection & Response - Cible de sécurité EDR - HarfangLab* Référence : DTU-2-05-CIBLE ; Version 2 ; Date : 18/08/2020.
[RTE]	*Rapport Technique d'Évaluation CSPN HURUKAI* Référence : Hurukai_CSPN_RTE ; Version : 1.4 ; Date : 15 décembre 2020.
[GUIDES]	*Documentation d'administration EDR HarfangLab* Référence : DTU-2-03-ADMIN ; Version : 1.5 ; Date : 10/09/2020. *Documentation d'installation EDR HarfangLab* Référence : DTU-2-01-INSTALL ; Version : 12.1 ; Date : 18/08/2020. *Documentation utilisateur EDR HarfangLab* Référence : DTU-2-02-USER ; Version : 1.4 ; Date : 24/06/2020.

ANNEXE B. Références 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-01/2.1 du 13 janvier 2020 ; Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019 ; Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. Documents disponibles sur www.ssi.gouv.fr.