EDR HARFANGLAB

ENDPOINT DETECTION & RESPONSE

CIBLE DE SECURITE

Ref: DTU_2-0-CIBLE_05 du 24-06-2020

REVISION DU DOCUMENT			
VERSION	DATE	AUTEUR	COMMENTAIRE
1.2	24/06/2020	HarfangLab	Version initiale

REVISION DU DOCUMENT		
ID	OBJET	REFERENCE
[NOTE/20]	Règles relatives à la mise en œuvre des évaluations sécuritaires	www.ssi.gouv.fr
[NOTE/21]	Méthodologie pour l'évaluation d'une gamme de produits	www.ssi.gouv.fr
[CSPN-CER-I-02]	Critères pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau	www.ssi.gouv.fr
[CSPN-NOTE/01]	Méthodologie pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau - Contenu du RTE	www.ssi.gouv.fr

TABLE DES MATIERES

TABLE DES ILLUSTRATIONS

1. AVANT PROPOS

1.1. Objet du document

Ce document constitue la cible de sécurité pour l'évaluation du logiciel « Agent EDR » de l'éditeur HarfangLab.

1.2. Références et version de la cible d'évaluation

Nom de l'éditeur	HarfangLab
Nom du produit	Agent EDR
N° de version	2.0
Domaine technique CSPN	Logiciel

1.3. Procédure d'identification du produit évalué

L'identification de la version du produit se fait en examinant les propriétés de dans le dossier d'installation de l'agent (clic droit puis « Propriétés »).

L'onglet « Détails » comporte un champ « Version du produit ». La capture suivante montre par exemple cet onglet dans une version en anglais de Windows :

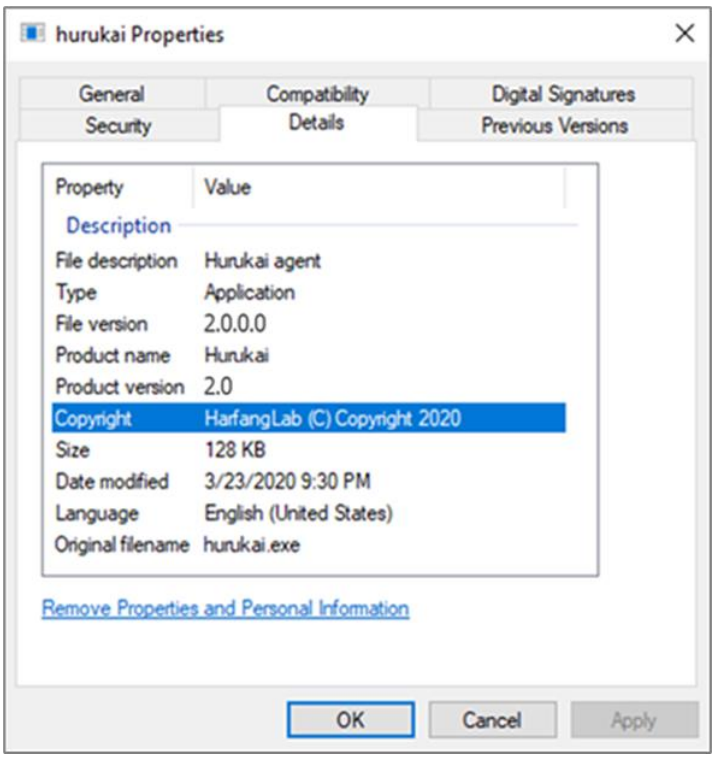

Figure 1 — Identification de la version produit

2. DESCRIPTION DU PRODUIT

Le produit objet de la présente cible de sécurité est l'agent logiciel utilisé dans la solution de l'EDR (« Endpoint Detection & Response ») de l'éditeur HarfangLab.

2.1. Description générale et fonctionnalités du produit

Cet agent est utilisé dans une solution plus globale dans un des scénarios d'utilisation suivant :

- observation permanente à des fins de détection d'intrusion et de réaction,
- réponse à incident et analyse.

L'agent comporte plusieurs fonctions locales hors périmètre d'évaluation telles que :

- la surveillance des processus,
- le relevé d'informations,
- le lancement de tâches depuis un centre d'administration distant.

Par rapport à ces fonctions locales, sont évalués :

- L'innocuité de l'agent, c'est-à-dire le fait que la présence de l'agent ne dégrade pas la sécurité des machines sur lesquelles il est déployé. Celle-ci s'appuie notamment sur les mécanismes de contrôle d'accès du système d'exploitation. L'évaluation de cette partie porte donc sur la bonne utilisation de ces mécanismes lors de l'installation de l'agent.
- L'auto-protection de l'agent en empêchant qu'un simple utilisateur ou qu'un administrateur local au poste ne puisse désactiver le service EDR ou désinstaller l'agent.

L'agent comporte également des fonctions permettant la communication avec le manager :

- Authentification du manager (par rapport à une autorité de certification racine),
- Protection de la confidentialité et de l'intégrité des données et des ordres échangés avec le manager.

Ces fonctions sont dans le périmètre d'évaluation. Pour cela, l'agent commence par monter un tunnel de transport via un tunnel TLS chiffré. Le tunnel est monté à l'initiative de l'agent et jamais à l'initiative du manager. L'identité du manager est vérifiée selon deux paramètres du certificat présenté par celui-ci :

- l'autorité de certification racine, comparée à une valeur codée en dur dans l'agent et évitant ainsi une usurpation du certificat du manager,
- la clé d'identification du manager (qui est en fait le condensat SHA-256 de sa clé publique, non lié à la négociation TLS), saisie lors de l'installation de l'agent.

Les données échangées sont ensuite encapsulées dans un protocole à base de données sérialisées via MessagePack et chiffrées authentifiées avec AES-128 et HMAC SHA-256. Les clés symétriques sont échangées et protégées via un échange basé sur l'algorithme Diffie-Hellman sur courbe elliptique et utilisant la clé publique du manager.

2.2. Description de l'utilisation du produit

La figure ci-dessous présente une architecture type de solution, illustrant l'intégration de l'agent avec son manager.

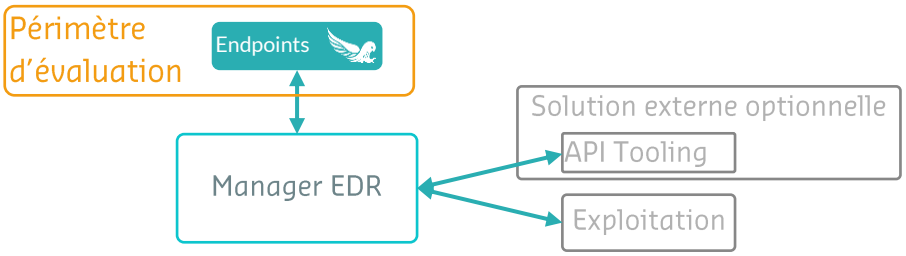

Figure 2 — Périmètre d'évaluation dans la solution

À noter : les flux présentés ci-dessus sont en HTTPS.

Le manager présente des conditions de déploiement qui lui sont propres et qui spécifient des mesures de sécurité visant à protéger les données et fonctions sensibles.

2.3. Plateforme d'évaluation du produit

La plateforme d'évaluation du produit est constituée d'une configuration standard de manager sous la forme d'une machine virtuelle, de l'agent sur une version de référence de Windows (la dernière version de Windows 10 disponible au début des tests) et de l'agent sur les autres versions de Windows supportées (identifié en section

3. ENVIRONNEMENT OPERATIONNEL DU PRODUIT

3.1. Utilisateurs du produit

Après l'installation locale de l'agent par un administrateur système de la machine concernée, l'agent est administré depuis le manager.

Aucune interaction n'a lieu avec les utilisateurs locaux. Les droits sur les agents font l'objet d'une politique de gestion des droits propre au manager.

3.2. Environnement d'exploitation du produit

Le produit évalué, le logiciel agent, s'intègre dans son environnement selon le principe illustré par la figure suivante :

Comme illustré ci-contre, l'agent est composé d'un service et d'un module noyau fonctionnant sous Windows

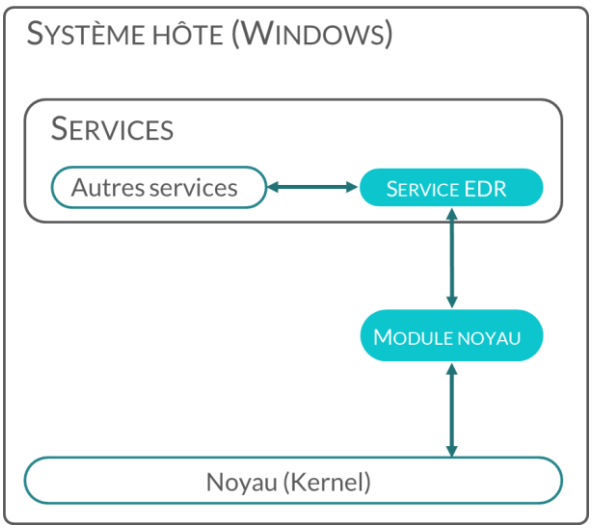

Figure 3 – Environnement technique du produit évalué

Les versions de Windows supportées par l'agent et considérées dans le support de l'évaluation sont :

- Windows 7 et versions ultérieures pour les postes utilisateurs ;
- Windows Server 2008 R2 et versions ultérieures pour les serveurs.

3.3. Hypothèses d'exploitation du produit

Il est pris pour hypothèse **[H1.Host]** le système d'exploitation ne doit pas nécessairement faire l'objet d'un durcissement, mais ne fait pas l'objet d'affaiblissement de sa sécurité par la configuration qui lui est appliquée ou l'utilisation qui en est faite. En particulier :

- Une séparation des rôles « utilisateur » et « administrateur » est mise en place. L'utilisation nominale est faite depuis un compte avec un rôle « utilisateur ».
- Une authentification robuste des utilisateurs et des administrateurs est mise en place.
- Le contrôle d'accès aux fichiers limite les droits en modification des fichiers du système d'exploitation et des programmes installés (dossier %PROGRAMFILES%).
- La séparation des privilèges d'accès aux ressources est mise en place, d'une part entre les espaces noyau et application, et d'autre part entre les différents processus s'exécutant dans ces espaces.

>> Aucune autre hypothèse n'est requise concernant la sécurisation du réseau de déploiement des agents.

3.4. Mesure de sécurité apportées par l'environnement du produit

Les mesures de sécurité mises en œuvre sur l'hôte de l'agent, détaillées en section précédente, protègent vis-à-vis d'un utilisateur standard de l'hôte ou d'un processus s'exécutant sur celui-ci :

- L'intégrité du logiciel de l'agent lui-même et de sa configuration.
- La confidentialité et l'intégrité des données en mémoire.
- L'intégrité d'exécution des processus de l'agent.

Le certificat du manager et la clé privée associée qui sont utilisés pour sécuriser les échanges sont générés lors du déploiement et sont protégés en confidentialité et en intégrité par les mesures de durcissement du « manager » et par les politiques de sécurité de l'organisation.

4. BIENS SENSIBLES

4.1. Biens utilisateur

Les biens utilisateur à protéger par l'agent sont :

- **B1.Collecte** : L'ensemble des données collectées par l'agent et utilisées pour la détection locale et l'envoi au manager. Ces données doivent être protégées en confidentialité et en intégrité.
- **B2.Ordre** : Les ordres envoyés par le manager à l'agent en vue de réaliser des opérations sur l'hôte. Ces données doivent être protégées en authenticité (dont l'anti-rejeu).

D'autres biens sensibles sont protégés par l'environnement de l'agent, comme détaillé en section suivante.

4.2. Biens du produit

Les biens du produit sont :

- **B3.Logiciel** : Le logiciel de l'agent.Ce bien est protégé :
  - en authenticité lors de l'installation (vérification de signature),
  - en intégrité hors exécution par le contrôle d'accès du système d'exploitation (hypothèse H1.Host),
  - en intégrité lors de l'exécution par les fonctions de sécurité du produit.
- **B4.Configuration** : La configuration de l'agent comportant notamment la clé d'identification du manager définie par l'opérateur réalisant l'installation. Ce bien est protégé :
  - oen intégrité hors exécution par le contrôle d'accès du système d'exploitation (hypothèse H1.Host),
  - en intégrité lors de l'exécution par les fonctions de sécurité du produit.
- **B5.Secrets cryptographiques** : Les clés de trafic TLS et autres secrets cryptographiques négociés lors de la connexion de l'agent avec le manager. Ces biens sont protégés en confidentialité et intégrité par le cloisonnement de processus du système d'exploitation hôte (hypothèse H1.Host) et par les fonctions de sécurité du produit.

4.3.Synthèse

TYPE DE BIEN	IDENTIFIANT	CONFIDENTIALITE	INTEGRITE	AUTHENTICITE
UTILISATEURS	**B1.Collecte**	Sécurisation des flux	Sécurisation des flux	
	B2.Ordre			Anti-rejeu
PRODUIT	**B3.Logiciel**		Contrôle d'accès OS	Vérification de signature
	B4.Configuration		Contrôle d'accès OS	
	B5.Secrets cryptographiques	Cloisonnement de processus	Cloisonnement de processus	

5. MENACES SUR LES BIENS A PROTEGER

Ce chapitre décrit les scénarios de menace sur les biens à protéger par le produit sous la forme : un agent menaçant *réalise une action* sur des **biens sensibles**. Les biens sensibles sont parfois fonctionnels comme par exemple **le comportement du produit** ou **le comportement de l'environnement du produit**. Lorsqu'aucune référence de bien n'est spécifiée, c'est que tous les biens sont potentiellement concernés.

5.1. Scénarios

M1. Compromission locale

Un attaquant local sans privilège *accède* à **des données confidentielles de l'agent**. Il peut par exemple tenter d'obtenir des secrets de chiffrement de disque ou des données d'un autre utilisateur de l'hôte.

M2. Altération locale sans privilèges

Un attaquant local sans privilège *accède* à l'agent pour *modifier* **le comportement de celui-ci** ou **le comportement de l'hôte**. Il peut par exemple tenter d'obtenir des privilèges par ce moyen. Cette menace ne concerne pas directement des biens protégés par l'agent.

M3. Écoute passive

Un attaquant sur le réseau *accède* à **des données confidentielles** échangées entre l'agent et le manager (B1). Il peut par exemple enregistrer le trafic réseau et attaquer le chiffrement a posteriori sur cet enregistrement.

M4. Intrusion réseau

Un attaquant sur le réseau *altère* **les données échangées** entre l'agent et le manager (B1 et B2) dans le but d'usurper le manager ou de *lancer* **des opérations non souhaitées sur l'agent**. Il peut par exemple usurper l'identité du manager pour lancer des scripts depuis l'agent afin de prendre le contrôle de l'hôte.

M5. Altération locale avec privilèges

Un attaquant local avec privilège *accède* à l'agent pour *modifier* **le comportement de celui-ci** ou **le comportement de l'hôte.** Il peut par exemple dissimuler un piratage de l'hôte ou de l'agent par ce moyen.

5.2. Synthèse des menaces

SOURCE DE MENACE	IDENTIFIANT	BIENS SENSIBLES	EVENEMENT REDOUTE
LOCALE SANS PRIVILEGE	M1.compromission locale	B1 à B5	Accès à des données confidentielles (secrets de chiffrement de disque ou d'autres utilisateurs)
	M2.altération locale sans privilèges	B1 à B5	Modification du comportement de l'agent (Gain de privilège)
LOCALE AVEC PRIVILEGE	M5.altération locale avec privilèges	B1 à B5	Modification du comportement de l'agent et de l'hôte (dissimuler une compromission)
ATTAQUANT SUR LE RESEAU	M3.écoute passive	B1	Accès à des données confidentielles (enregistrement du trafic réseau)
	M4.intrusion réseau	B1 & B2	Altération des données échangées (usurpation du manager ou lancement d'action sur l'agent)

6. SPECIFICATIONS DES FONCTIONS DE SECURITE

F1.Authentification manager

Lors de la configuration de l'agent à l'installation, une adresse de manager (collecteur) et une clé d'identification de celui-ci sont définies par l'opérateur réalisant l'installation.

Lors de la connexion, un tunnel HTTPS (HTTP dans TLS) est établi avec le manager qui s'authentifie au moyen d'un certificat x509. Ce certificat est vérifié par l'agent, notamment l'autorité de certification racine, par rapport à un certificat public embarqué dans le logiciel d'installation de l'agent.

Cette vérification est détaillée dans la description de la fonction de sécurité suivante.

F2. Confidentialité et intégrité du trafic utilisateur

Les données échangées entre l'agent et le manager sont protégées en confidentialité et en intégrité par cette fonction.

Pour cela, l'agent commence par monter un tunnel de transport via un tunnel TLS chiffré. Le tunnel est monté à l'initiative de l'agent et jamais à l'initiative du manager. L'identité du manager est vérifiée selon deux paramètres du certificat présenté par celui-ci :

- l'autorité de certification racine, comparée à une valeur codée en dur dans l'agent et évitant ainsi une usurpation du certificat du manager,
- la clé d'identification du manager (qui est en fait le condensat SHA-256 de sa clé publique, non lié à la négociation TLS), saisie lors de l'installation de l'agent.

Les données échangées sont ensuite encapsulées dans un protocole à base de données sérialisées via MessagePack et chiffrées authentifiées avec AES-128 et HMAC SHA-256. Les clés symétriques sont échangées et protégées via un échange basé sur l'algorithme Diffie-Hellman sur courbe elliptique et utilisant la clé publique du manager.

F3. Cloisonnement de l'exécution

Le but de cette fonction est de collecter des événements et de traiter les ordres du manager de manière sûre sans que les utilisateurs standards n'aient accès aux informations collectées ou aux ordres reçus. Pour cela, la fonction s'appuie sur les mécanismes de sécurité du système d'exploitation hôte en exécutant ses processus avec des niveaux de privilège interdisant à un utilisateur standard d'accéder aux données et à la mémoire de ces processus.

Il s'agit notamment du service EDR de l'agent qui s'exécute avec le compte SYSTEM et d'un module noyau accessible uniquement par le service EDR de l'agent.

F4. Protection de l'exécution

Le but de cette fonction est de renforcer la fonction précédente de sorte que les utilisateurs privilégiés ne puissent pas non plus modifier le comportement de l'agent malgré leurs privilèges sur l'hôte.

Il s'agit notamment du service EDR de l'agent qui s'exécute avec le compte SYSTEM et d'un module noyau accessible uniquement par le service EDR de l'agent, comme illustré par la figure 3.

7. COUVERTURE DES MENACES

Le tableau ci-dessous illustre la couverture des menaces par les fonctions de sécurité du produit :

MENACE/FONCTION DE SÉCURITÉ	F1. AUTHENTIFICATION MANAGER	F2. CONFIDENTIALITE ET INTEGRITE DU TRAFIC UTILISATEUR	F3. CLOISONNEMENT DE L'EXÉCUTION	F4. PROTECTION DE L'EXÉCUTION
M1.Compromission locale			X	
M2.Altération locale sans privilèges			X	
M3.Ecoute passive	X	X		
M4.Intrusion réseau	X	X		
M5. Alteration locale avec privileges				X