CIBLE DE SÉCURITÉ CSPN

WAPT Enterprise v2.6.0.16859

Catégorie : Administration et supervision de la sécurité

Référence : *2024_CSPN_WAPT_tranquil-it_TOE*

Date : 18 juin 2026

Révision	Date	Description	Rédacteur(s)
1.00	12/09/2022	Création du document	Vincent CARDON, Denis CARDON
1.01	09/01/2023	Révision du document	Vincent CARDON, Denis CARDON
1.02	20/02/2023	Révision du document	Vincent CARDON, Hubert TOUVET
1.03	05/05/2023	Révision du document	Hubert TOUVET
1.04	29/06/2023	Révision du document, mise à jour des COTS	Vincent CARDON, Hubert TOUVET
1.05	29/09/2023	Révision du document, mise à jour des COTS, ajout des liens de documentation d'installation. Suppression autoprotection des librairies python.	Vincent CARDON, Hubert TOUVET
1.06	03/10/2023	Mise à jour module *python-engineio 4.7.1*. Suppression du patch *python-engineio*. Analyse des vulnérabilités des modules python. Suppression des modules *gitpython*, *gitdb* et *pykerberos*.	Denis CARDON, Hubert TOUVET
1.07	03/06/2024	Seules les données d'inventaires stockées sur le serveur sont un bien sensible. Passage OS machine management / client de Windows 10 à Windows 11	Denis CARDON, Hubert TOUVET
1.08	18/10/2024	TOE suite à l'analyse d'impact différentielle	Vincent CARDON, Hubert TOUVET
1.09	29/11/2024	Suite revue par l'ANSSI Ajout des références aux documents de référence. Précisions sur l'évaluation des fonctions désactivées.	Vincent CARDON, Hubert TOUVET
1.10	18/12/2024	Mise à jour des COTS	Hubert TOUVET, Denis CARDON
1.11	03/10/2025	Mise à jour des COTS	Hubert TOUVET, Denis CARDON
1.12	04/02/2026	Ajout COTS *innosetup* Mise à jour COTS Adaptation du document à **Note#09**	Hubert TOUVET, Denis CARDON, Vincent CARDON

Révision	Date	Description	Rédacteur(s)
1.13	13/02/2026	Mise à jour COTS Mise à jour version Wapt 2.6.0.16840	Hubert TOUVET
1.14	18/05/2026	Mise à jour documentaire	Hubert TOUVET
1,15	15/06/2026	Mise à jour COTS Mise à jour version Wapt 2.6.0.16856	Hubert TOUVET
1.16	18/06/2026	Mise à jour COTS Mise à jour version Wapt 2.6.0.16859	Hubert TOUVET

Ce document a été validé par Tranquil IT.

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma **CSPN** promu par l'ANSSI, du produit **WAPT Enterprise** développé par la société **Tranquil IT**.

TABLE DES MATIÈRES

INDEX DES FIGURES

INDEX DES TABLEAUX

1. OBJET DE L'ÉVALUATION

1.1. [E_CSPN_ST_4] Périmètre inclus dans la cible d'évaluation

L'évaluation porte sur :

- un *serveur WAPT waptserver* ;
- un *agent WAPT*, avec *waptexit* activé;
- la console de management *waptconsole* ;
- les communications réseau entre ces différentes composantes.
- la gestion sécurisée des paquets WAPT :
  - déploiement sécurisé d'un ou de plusieurs paquets WAPT ;
  - déploiement sécurisé d'une mise à jour d'un paquet WAPT ;
  - désinstallation d'un paquet WAPT.

La gestion sécurisée repose sur l'utilisation de certificats différenciés entre le gestionnaire de déploiement (certificat X509 standard) et le concepteur de paquets WAPT (certificat X509 avec l'attribut Code-Signing).

Les opérations qui font partie du périmètre externe de la TOE, et qui donc ne font pas partie du périmètre de l'évaluation sont :

- La rédaction en python du script WAPT ainsi que la fourniture de tous les autres fichiers servant à constituer le paquet WAPT.
- La gestion des clés privées de signature des paquets et la gestion et la révocation des certificats SSL.

1.2. [E_CSPN_ST_5] Identification du produit

Nom commercial du produit	WAPT
Numéro de la version évaluée	WAPT Enterprise v2.6.0.16859

1.2.1. Description des dépendances

L'installeur de l'agent WAPT embarque avec lui les dépendances nécessaires, c'est-à-dire l'interpréteur python et sa librairie standard, les librairies tierces nécessaires pour WAPT, les sources python spécifiques, les librairies openssl, et les runtime Microsoft C.

Le fonctionnement de WAPT sur le poste client n'est pas dépendant d'un environnement déjà installé, en dehors du système Windows lui-même.

1.2.2. Références

Pour l'établissement de la présente cible de sécurité, les documents suivants ont été consultés par le rédacteur :

- https://wapt.tranquil.it/ : store de paquets officiels ;
- https://www.wapt.fr/fr/doc-2.6/ : documentation officielle du produit.
- ANSSI-CSPN-CER-P-01_v5.0 : Procédure de Certification de Sécurité de Premier Niveau (CSPN) des produits des technologies de l'information.
- ANSSI-CSPN-NOTE-09 : contenu et structure de la cible de sécurité CSPN.

1.2.3. Documentation d'installation

- Installation du serveur : https://www.wapt.fr/fr/doc-2.6/wapt-server-install-redhat-based.html

- Points spécifiques à la TOE: https://www.wapt.fr/fr/doc-2.6/wapt-server-install-redhat-based.html#cspn-mode-post-configuration
- Installation console de gestion et agents : https://www.wapt.fr/fr/doc-2.6/wapt-configuration.html

2. USAGES DU PRODUIT WAPT

2.1. [E_CSPN_ST_6] Description détaillée et usage attendu du produit

WAPT automatise l'installation, la (post)configuration, la mise à jour et la suppression de logiciels sur un parc Windows, Linux et macOS. Le déploiement de logiciels (Firefox, MS Office, ...) s'effectue de manière centralisée avec la console graphique. Le fonctionnement de WAPT s'inspire fortement du gestionnaire de paquets du système GNU / Linux Debian *apt*, d'où le nom WAPT.

WAPT est constitué de trois sous-ensembles :

2.1.1. Composante serveur

La composante serveur est elle-même découpée en deux composantes hébergées sur une machine unique ou un jeu de machines physiques ou virtuelles :

- Un *waptserver* qui stocke de manière centralisée l'inventaire du parc. En complément, il sert à notifier les agents WAPT d'opérations immédiates.
- Un ou plusieurs *waptrepo* qui stockent les paquets WAPT sur le système de fichiers local, les paquets groupe, les paquets selfservice, les paquets d'unités organisationnelles, les paquets de configuration des mises à jour Windows et les paquets machine.

2.1.2. Composante client

La composante client est elle-même découpée en deux sous-composantes obligatoires et trois sous-composantes optionnelles :

- Un exécutable *wapt-get* obligatoire qui gère une copie locale des paquets disponibles et le processus d'installation et de mise à jour des logiciels à partir de ce dépôt local. *wapt-get* permet également d'interagir avec le webservice local *waptservice*.
- un service *waptservice* obligatoire dont le rôle est d'interroger à intervalles réguliers son ou ses dépôts distants pour savoir si de nouvelles mises à jour existent. Ce service gère aussi un service web à l'adresse https://localhost:8088 qui permet aux composants *wapt-get*, *waptself*, *wapttray* et *waptexit* d'interagir localement avec le *waptservice* local.
- un exécutable *wapttray* optionnel fonctionnant en espace utilisateur qui installe une icône dans la barre de notification du client Windows affichant des informations à l'utilisateur connecté. Le *wapttray* interagit uniquement avec le *waptservice* local.
- un exécutable *waptexit* optionnel s'exécutant lorsque le poste est en phase d'arrêt et permettant à l'Utilisateur de choisir ou non d'installer les mises à jour proposées par WAPT avant d'éteindre la machine. Le *waptexit* interagit uniquement avec le *waptservice* local.
- un exécutable *waptself* optionnel permettant à l'Utilisateur d'installer des paquets proposé par l'Administrateur métier WAPT. Le *waptself* interagit uniquement avec le *waptservice* local.

2.1.3. Composante console

La console d'administration *waptconsole* est installée sur le poste d'administration de l'Administrateur métier WAPT. Elle fournit à l'Administrateur métier un environnement graphique convivial pour :

- déployer et supprimer des paquets sur les cibles de son choix ;
- dupliquer des paquets depuis des dépôts externes et les importer dans son dépôt privé ;
- contrôler le bon déroulement des opérations de gestion de parc.

La sécurité de WAPT est basée sur la signature asymétrique des paquets. Seuls les paquets signés avec la clé privée de l'Administrateur métier pourront être installés sur les postes clients équipés de la clé publique de l'Administrateur métier. La console permet d'importer des paquets depuis des dépôts tiers ; l'Administrateur métier vérifie, valide et signe avec sa clé privée le paquet WAPT récupéré avant de le pousser vers son dépôt privé. La rupture de responsabilité se passe à cette étape

quand un Administrateur métier récupère un paquet depuis une source publique.

L'installeur de l'agent WAPT est généré par l'Administrateur métier depuis la console d'administration. Ceci permet d'intégrer au binaire d'installation de l'agent la clé publique associée à la clé de signature du serveur, ainsi que d'autres informations de configuration (URL du serveur, etc.). Les agents WAPT sont déployés sur le parc manuellement ou de manière automatisée (ex : GPO, Intune ou autre moyen). Les mises à jour de l'agent WAPT sont également déployées via WAPT.

Les agents WAPT sont authentifiés initialement sur le serveur au moyen de Kerberos. Lors de la première connexion au serveur, l'authentification est déléguée à Kerberos afin de permettre à l'agent d'envoyer son certificat au serveur. Les authentifications suivantes sont réalisées sans Kerberos.

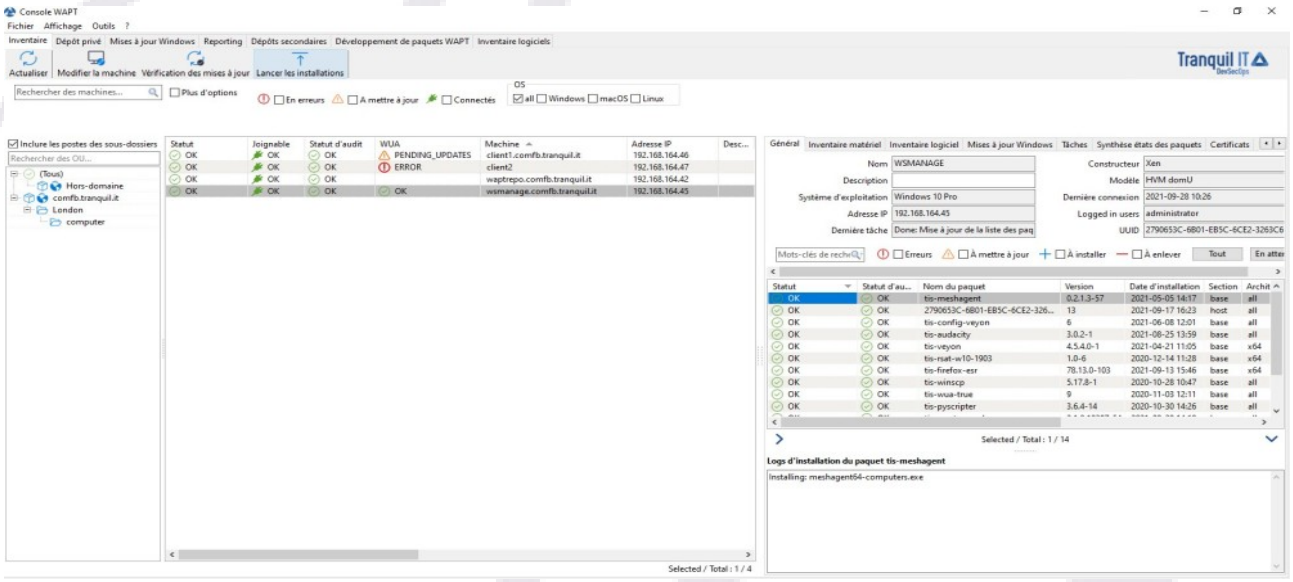

Figure 1: Capture d'écran de la console WAPT

2.1.4. Principe de fonctionnement

L'installeur du serveur WAPT est téléchargeable à l'adresse suivante :

https://wapt.tranquil.it/wapt/releases/tis-waptserver-2.6.0.16859-d3e86c84.x86_64.rpm

L'Administrateur métier doit :

- définir un mot de passe pour se connecter au serveur WAPT depuis la console ;
- générer un certificat pour la protection des paquets à déployer.

Les paramètres de configuration de l'agent sont définis dans le fichier *wapt-get.ini*. Les paramètres de la console *waptconsole* sont définis dans le fichier utilisateur *%LOCALAPPDATA%\waptconsole\waptconsole.ini*.

Pour installer les agents sur les postes distants, l'Administrateur de la solution doit générer l'installeur de l'agent depuis la console d'administration du serveur. Ceci permet de configurer automatiquement l'agent avec les informations relatives au serveur (URL d'accès, clé publique du certificat, etc.). L'agent WAPT peut être installé et mis à jour directement sur les postes par une méthode choisie par les Administrateurs Locaux des machines (déploiement par GPO avec l'exécutable *waptdeploy*, ou toute autre manière).

WAPT peut s'utiliser via l'interface graphique *waptconsole* ou au travers du *self-service*, ou encore en ligne de commande (ex : *wapt-get install tis-firefox*).

En ligne de commande sur l'agent, les commandes principales sont les suivantes :

- La commande `wapt-get update` permet de mettre à jour la liste des paquets disponibles.

- La commande `wapt-get list` permet de lister les paquets installés sur la machine.
- La commande `wapt-get search <nom du paquet>` permet de chercher un paquet sur un dépôt.
- La commande `wapt-get install <nom du paquet>`.
- La commande `wapt-get remove <nom du paquet>` permet de désinstaller un logiciel.
- La commande `wapt-get upgrade` permet d'installer tous les paquets en attente de mise à jour.

Le serveur peut être installé sous Debian / Redhat et leurs dérivées ou Windows (Windows 10 et supérieur, Windows Server 2012R2 et supérieur) en architecture 64 bits.

Les agents sont disponibles pour les systèmes Windows (7 à 11 et Server 2003 à 2022), les systèmes Debian / Redhat et leurs dérivés, et enfin pour macOS High Sierra et supérieurs.

La console d'administration est un client natif disponible sur les systèmes Windows, Linux et macOS.

2.2. [E_CSPN_ST_7] Concepteur du produit

Éditeur	Tranquil IT 12, avenue Jules Verne 44230 Saint Sébastien Sur Loire, France
Lien vers l'organisation	https://tranquil.it/

2.3. [E_CSPN_ST_8] Domaine technique

Domaine technique	Administration et supervision de la sécurité

3. ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT DU PRODUIT

3.1. [E_CSPN_ST_9] Environnement du produit

L'évaluation portera sur :

- Le serveur WAPT (*waptserver*) installé sur Rocky Linux 10 à jour (clone de RedHat 10) avec *SELinux* et *firewalld* activés.
- Un agent WAPT installé sur Windows 11 à jour de ses derniers patchs.
- La console de management (*waptconsole*) installée sur Windows 11.

La console est connectée au serveur WAPT au travers d'un réseau local. Ce poste hébergeant la console peut disposer également d'un accès à un réseau non maîtrisé au travers duquel il obtient des paquets (des logiciels ou leurs mises à jour) que l'Administrateur métier souhaite ensuite intégrer à son dépôt WAPT privé.

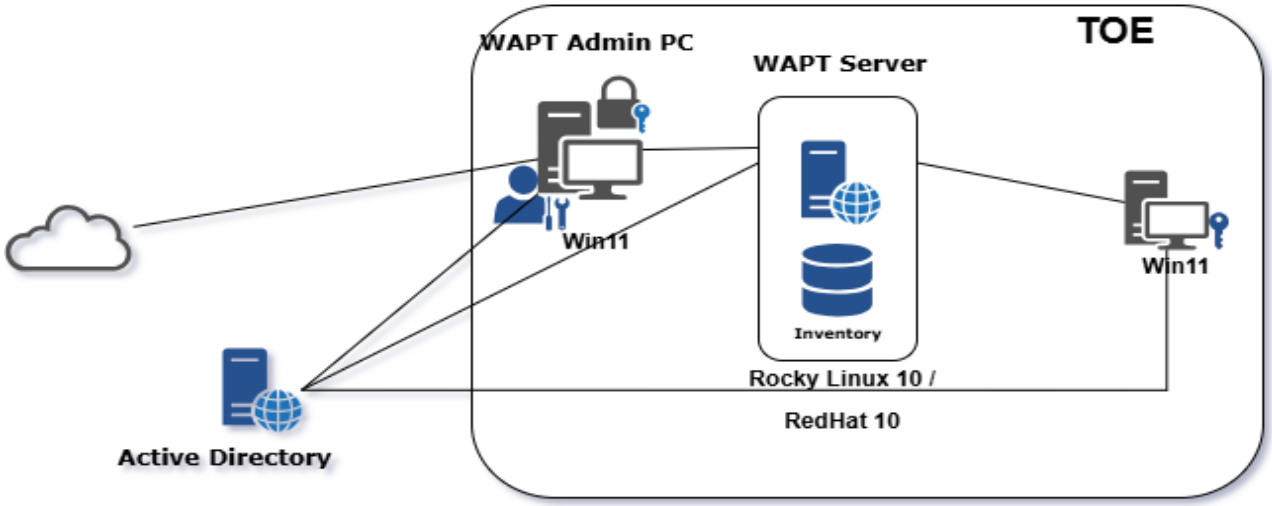

Figure 2: Cible d'évaluation

Les postes de travail et la console d'administration de la plateforme d'évaluation sont joints à un domaine d'authentification de type Active Directory.

Le fonctionnement de WAPT sur les plateformes clientes (agent, console d'administration) Linux et macOS ne sera pas évalué.

Le fonctionnement de WAPT sur les plateformes clientes (agent, console d'administration) Linux et macOS ne sera pas évalué.

Le certificat HTTPS du serveur *Nginx* utilisé lors de l'évaluation est un certificat auto-signé et généré lors de l'installation de WAPT. Il est déployé en même temps que les agents et est épinglé avec le certificat du serveur WAPT.

3.2. [E_CSPN_ST_10] Éléments de l'environnement et attaquants potentiels

Composant du système global			Inclus dans le produit évalué	Non évalué (environnement du produit)	
				Supposé de confiance	Est un attaquant potentiel
A - Machine administrée par WAPT ou machine de l'administrateur WAPT	**C_A.1**	Matériel et micrologiciel	Non	Oui	Non
	C_A.2	Système d'exploitation	Non	Oui	Non
	C_A.3	Applicatif (le produit WAPT)	Oui	N/A	N/A
B - Serveur WAPT	**C_B.1**	Matériel et micrologiciel	Non	Oui	Non
	C_B.2	Système d'exploitation	Non	Oui	Non
	C_B.3	Applicatif (le produit WAPT)	Oui	N/A	N/A
C – Active Directory	**C_C.1**	Annuaire d'entreprise	Non	Oui	Non

3.3. [E_CSPN_ST_11] Dépendances et composants tiers (COTS)

Tableau 1: Composants tiers intégrés au produit

Composant	Version	à jour de la dernière version	Maintenue	Origine
Serveur WAPT composants OS				
Nginx	1.26.3	Oui (distrib)	Oui (distrib)	Distribution RHEL10 à jour
Serveur PostgreSQL	16.11	Oui (distrib)	Oui (distrib)	Distribution RHEL10 à jour
Librairie kerberos MIT (pour module spnego et msktutil)	1.21.3	Oui (distrib)	Oui (distrib)	Distribution RHEL10 à jour
msktutil	1.2.2	Oui (distrib)	Oui (distrib)	Distribution RHEL10 à jour
nginx-mod-http-auth-spnego	1.26.3	Oui (upstream)	Oui (upstream)	compilé depuis les sources nginx et https://github.com/stnoonan/spnego-http-auth-nginx-module (hash git 005723a)
Serveur WAPT composants Python et librairies Partagées				
python 3.10	3.10.20	Oui (upstream branche 3.10)	Oui (upstream branche 3.10)	compilé depuis les sources https://www.python.org/ftp/python/3.10.20/Python-3.10.20.tgz
libffi sous Linux	3.5.2	Oui (upstream)	Oui (upstream)	Compilé depuis les sources https://github.com/libffi/libffi/releases/download/v3.5.2/libffi-3.5.2.tar.gz

libffi sous Windows	3.5.3	Non (version max supportée par Python en ABI7)	Oui (upstream Python)	Compilé depuis les sources https://github.com/libffi/libffi/releases/download/v3.5.2/libffi-3.5.2.tar.gz
openssl	3.5.7	Oui (upstream branche 3.5)	Oui (upstream branche 3.5)	Compilé depuis les sources https://github.com/openssl/openssl/releases/download/openssl-3.5.7/openssl-3.5.7.tar.gz
zlib sous Windows	1.3.2	Oui (upstream)	Oui (upstream)	Compilé depuis les sources https://zlib.net/zlib-1.3.2.tar.gz
sqlite	3.53.2	Oui (upstream)	Oui (upstream)	Compilé depuis les sources https://sqlite.org/2026/sqlite-autoconf-3530200.tar.gz
readline	8.3	Oui (upstream)	Oui (upstream)	Compilé depuis les sources https://ftp.gnu.org/gnu/readline/readline-8.3.tar.gz
gdbm	1.26	Oui (upstream)	Oui (upstream)	Compilé depuis les sources https://ftp.gnu.org/gnu/gdbm/gdbm-1.26.tar.gz
krb5 sous Linux (pour les binaires Wapt)	1.22.2	Oui (upstream)	Oui (upstream)	Compilé depuis les sources https://web.mit.edu/kerberos/dist/krb5/1.22/krb5-1.22.2.tar.gz
libp11 sous Linux	0.4.16	Oui (upstream)	Oui (upstream)	Compilé depuis les sources https://github.com/OpenSC/libp11/releases/download/libp11-0.4.18/libp11-0.4.18.tar.gz
libxcrypt sous Linux	4.5.2	Oui (upstream)	Oui (upstream)	Compilé depuis les sources https://github.com/besser82/libxcrypt/releases/download/v4.5.2/libxcrypt-4.5.2.tar.xz
libnsl sous Linux	2.0.1	Oui (upstream)	Oui (upstream)	Compilé depuis les sources https://github.com/thkukuk/libnsl/releases/download/v2.0.1/libnsl-2.0.1.tar.xz
Libpq (lib postgresql pour psycopg2) sous Linux	15.18	Oui (upstream branche 15.x)	Oui (upstream branche 15.x)	Compilé depuis les sources https://ftp.postgresql.org/pub/source/v15.18/postgresql-15.18.tar.gz
Libtirpc	1.3.7	Oui (upstream)	Oui (upstream)	Compilé depuis les sources https://downloads.sourceforge.net/libtirpc/libtirpc-1.3.7.tar.bz2
Modules python	**voir ci-dessous pour la liste**			installés par la commande pip
Binaires spécifiques WAPT : waptconsole, wapt-get, waptexit, wapttray, waptdeploy, waptlicences				
Lazarus 4.2	4.2 hash ada7a90f86	Oui (upstream)	Oui (upstream)	https://gitlab.com/freepascal.org/lazarus/lazarus.git/
freepascal 3.2	3.2	Oui (upstream)	Oui (upstream)	https://gitlab.com/freepascal.org/fpc/source.git/
mormot2	2.3 Git Sha1 `5a38c854c7b82d0b53fa95dea0e5d7354396b443`	Oui (upstream)	Oui (upstream)	https://github.com/synopse/mORMot2

3.3.1. Modules python agent et serveur

Les modules Python sont importés sous forme de source depuis pypi.org et compilés sous forme de *wheel* et conservés sur un dépôt *pip* interne. La ferme de build WAPT ne fait pas de connexion directe vers internet pour les installations de modules Python.

La colonne « Plateforme cible » indique des paquets *wheel* qui ne sont installés que sur certaines architectures cibles.

Tableau 2: Modules Python communs aux Agents et au Serveur WAPT Windows et Linux

Modules Python communs aux Agents et au Serveur	Version	Remarques
arpy	2.3.0	
babel	2.18.0	
beautifulsoup4	4.15.0	
bidict	0.23.1	
blinker	1.9.0	
certifi	2026.5.20	
cffi	2.0.0	
chardet	7.4.3	
charset-normalizer	3.4.7	
cheroot	11.1.2	
click	8.4.1	
configparser	7.2.0	
cryptography	46.0.7	
decorator	5.3.1	
distro	1.9.0	
eventlet	0.40.4	
flask	3.1.3	
flask-socketio	5.6.1	
future	1.0.0	
gnureadline	8.3.3	
greenlet	3.5.1	
h11	0.16.0	
idna	3.18	
importlib-metadata	9.0.0	
iniparse	0.5	
ipaddress	1.0.23	
itsdangerous	2.2.0	
jaraco-functools	4.5.0	
jinja2	3.1.6	
markupsafe	3.0.3	
more-itertools	11.1.0	

Modules Python communs aux Agents et au Serveur	Version	Remarques
psutil	7.2.2	
psycopg2	2.9.12	
pycparser	3.0	
pyparsing	3.3.2	
python-engineio	4.13.2	
python-pam	2.0.2	
python-socketio	5.16.2	
pywin32	312	
requests	2.34.2	
rpmfile	2.2.1	
setproctitle	1.3.7	
simple-websocket	1.1.0	
six	1.17.0	
smmap	5.0.3	
soupsieve	2.8.4	
typing_extensions	4.15.0	
ujson	5.12.1	
urllib3	2.7.0	
wakeonlan	3.3.0	
websocket-client	1.9.0	
werkzeug	3.1.8	
winsys	1.2	
wmi	1.5.1	
wsproto	1.3.2	
zipp	4.1.0	
setuptools	82.0.1	

Tableau 3: Modules Python spécifiques au Serveur WAPT

Modules Python spécifiques au Serveur	Version	
babel	2.18.0	
bidict	0.23.1	
blinker	1.9.0	
cachelib	0.14.0	
click	8.4.1	
dnspython	2.8.0	
eventlet	0.41.0	
flask	3.1.3	
flask-babel	4.0.0	
flask-session	0.8.0	
flask-socketio	5.6.1	
greenlet	3.5.1	
h11	0.16.0	
hashring	1.5.1	
huey	3.0.1	
itsdangerous	2.2.0	
jinja2	3.1.6	
markupsafe	3.0.3	
monotonic	1.6	
msgspec	0.21.1	
passlib	1.7.4	
peewee	3.19.0	
psycogreen	1.0.2	
psycopg2	2.9.12	
python-engineio	4.13.2	
python-socketio	5.16.2	
simple-websocket	1.1.0	
urllib3	2.7.0	

uwsgi	2.0.31	
werkzeug	3.1.8	
wsproto	1.3.2	

3.3.2. Correctifs spécifiques

Tableau 4: Ajouts / Correctifs spécifiques WAPT pour les modules python

Module python	Version	Description
iniparse	0.5	Le mot clé REM (remarque) doit être suivi d'un espace pour être une remarque

3.3.3. Vulnérabilités connues

Tableau 5: Vulnérabilités connues

Composant	Description
python 3.10	https://www.cert.ssi.gouv.fr/avis/CERTFR-2026-AVI-0079/ WAPT n'utilise pas le paramètre *altchars* dans la fonction *base64.b64decode* ni la fonction *urlsafe_b64decode*. Cette CVE n'augmente donc pas la surface d'attaque des fonctions de sécurité de WAPT. L'attaque par corruption de données d'entrée encodées en *base64* en y introduisant des caractères non inclus dans l'alphabet standard n'est pas différente de la corruption d'un autre attribut de paquet WAPT ou d'une action distante.

4. PROBLÈMES DE SÉCURITÉ

Attention : Le service WAPT fonctionne en compte système privilégié.

Un exploitant de WAPT devra choisir et suivre une méthodologie adaptée pour :

- Assurer un téléchargement sûr de tous les autres fichiers servant à constituer un paquet WAPT.
- Rédiger le script *python* `setup.py` d'installation d'un paquet WAPT de telle manière à éviter toute faille de sécurité ou de confidentialité exploitable.
- Gérer de manière sûre les clés privées de signature des paquets.
- Gérer de manière sûre les Autorités de Certification et de révocation des certificats SSL et HTTPS.

4.1. [E_CSPN_ST_12] Biens sensibles

4.1.1. (B1) Paquets WAPT

Les paquets WAPT à déployer sont un les principaux biens sensibles à protéger. Ils doivent être protégés en disponibilité sur le dépôt, et en intégrité lors du déploiement.

Besoin de sécurité : intégrité, authenticité, disponibilité

4.1.2. (B2) Actions déclenchées sur le poste client depuis la console

Des actions sont envoyées sur les agents depuis la console (via une payload json signée). Ces actions peuvent être la mise à jour du poste, le déploiement / désinstallation d'un paquet particulier, le redémarrage des machines, etc. Ces actions sont un bien sensible et doivent être protégées en intégrité et authenticité.

Besoin de sécurité : intégrité, authenticité

4.1.3. (B3) Matériel cryptographique

Le matériel cryptographique est un bien sensible et doit être protégé. Il sert de données d'authentification, il est utilisé pour le chiffrement.

Besoin de sécurité : intégrité, confidentialité, disponibilité

- la clef privée du serveur pour la communication https.
- la clef privée du poste correspondante au certificat de l'agent WAPT.
- la clef privée de l'administrateur WAPT correspondant au certificat de l'administrateur WAPT de type **code-signing**.
- la clef privée de l'administrateur WAPT correspondant au certificat de l'administrateur WAPT de type **non-code-signing**.
- le mot de passe de l'administrateur WAPT pour se connecter au serveur WAPT.
- les token kerberos de l'administrateur WAPT (service ticket pour le serveur WAPT).

Besoin de sécurité : intégrité, disponibilité

- le certificat du serveur pour la communication https.
- le certificat de l'agent WAPT : certificat signé par le serveur WAPT suite à une *CSR* par le poste authentifié.
- le certificat de l'administrateur WAPT de type **code-signing**.
- le certificat de l'administrateur WAPT de type standard **non-code-signing**.

4.1.4. (B4) Les communications

Les communications entre le serveur central et les agents ainsi que les communications entre la console et le serveur sont un bien sensible et doivent être protégées.

Besoin de sécurité : intégrité, confidentialité, authenticité.

4.1.5. (B5) Les données d'inventaire

Les informations sur l'état de déploiement des paquets, ainsi que configuration matérielle et logicielle des postes clients **stockées sur le serveur WAPT** sont un bien sensible et doivent être protégées.

Besoin de sécurité : intégrité, confidentialité.

4.1.6. (B6) Les journaux

Les journaux générés par WAPT sur le serveur central et les agents sont un bien sensible et doivent être protégés.

Besoin de sécurité : intégrité, disponibilité, confidentialité.

4.1.7. (B7) Les valeurs de configuration

Les valeurs de configuration du serveur dans les répertoire */opt/wapt/conf* et */opt/wapt/waptserver/ssl* (clés du serveur https, configuration accès à la base de données, configuration de l'authentification au serveur) sont un bien sensible et doivent être protégées.

Besoin de sécurité : intégrité, confidentialité, disponibilité.

4.1.8. (B8) Les exécutables WAPT installés

Les exécutables WAPT installés sur les postes client managés (contenu du répertoire *wapt* incluant les binaires, les dll, les fichiers de configuration et la base de données) sont un bien sensible et doivent être protégés.

Besoin de sécurité : intégrité.

4.1.9. (B9) Le système hôte

Les systèmes hôtes qui comprennent ici le serveur hébergeant le serveur WAPT, les postes d'administration hébergeant les console d'administration et les postes utilisateurs équipés de l'agent WAPT sont un bien sensible et doivent être protégées.

Besoin de sécurité : intégrité, confidentialité, disponibilité.

4.2. Mesures d'environnement

4.2.1. [E_CSPN_ST_13] Utilisateurs et entités interagissant avec le produit

Tableau 6: Description des attaquants et niveaux de confiance

ID	Description de l'acteur	Degré de confiance
A1	**Utilisateur final** Un Utilisateur est un individu équipé d'une machine avec l'agent WAPT. Il peut mettre à jour son poste en fonction du paramétrage défini par le gestionnaire de déploiement.	**Attaquant potentiel**
A2	Administrateur métier : **Gestionnaire de déploiement** Un Gestionnaire de déploiement est un Administrateur Métier pouvant signer des paquets NE CONTENANT PAS de code python (en général les paquets de type profile group, unit et host) et les charger sur le dépôt principal. Il définit des profils de déploiement (ensemble de paquets WAPT affectés à des postes de travail) Il est identifié par l'absence de l'attribut Code-Signing de son certificat.	**De confiance**
A3	Administrateur métier : **Développeur de paquet** Un Développeur de Paquet est un Administrateur Métier pouvant signer des paquets, que les paquets CONTIENNENT OU NON du code python et les charger sur le dépôt principal. Le développeur de paquets est identifié par l'attribut Code-Signing de son certificat.	**De confiance**
A4	Administrateur métier : **SuperAdmin** Le SuperAdmin est un Administrateur Métier avec tous les droits dans WAPT. Il définit notamment les ACL, crée les autres autres administrateurs.	**De confiance**

ID	Description de l'acteur	Degré de confiance
A5	Administrateur système : **Administrateur Local** Un Administrateur système est un Administrateur Local disposant des droits d'administration locaux sur les postes équipés de WAPT. Il est utilisé pour faire le déploiement initial d'agent WAPT au besoin.	**De confiance**
A6	**Machines équipées de l'agent WAPT** Une machine équipée d'un agent WAPT est configurée pour interagir avec le serveur WAPT.	**De confiance**
A7	**Active Directory**	**De confiance**
A8	**RSSI**	**De confiance**
A9	**Attaquant sur le réseau**	**Attaquant potentiel**

4.3. [E_CSPN_ST_14] Produit livré sous forme physique

Néant, WAPT est strictement un logiciel hébergé sur l'infrastructure de son exploitant.

4.4. [E_CSPN_ST_15] Accès distant de l'éditeur au produit

Néant, Tranquil IT ne maintient **aucun** accès distant au produit WAPT hébergé par son exploitant.

4.5. [E_CSPN_ST_16] Mesures environnementales

Les hypothèses suivantes sur l'environnement d'exploitation de WAPT doivent être considérées :

Tableau 7: Hypothèses sur l'environnement d'exploitation

ID	Type de mesure	Description de la mesure	Acteurs en charge de la mesure
H1	Organisationnelle	Les administrateurs métier sont de confiance et formés à l'usage de WAPT. En particulier, ils doivent s'assurer que leurs identifiants et clés de sécurité restent secrets et protégés.	RSSI (**A8**) Tous les administrateurs (**A2**, **A3**, **A4**, **A5**)
H2	Organisationnelle	Les systèmes d'exploitation sur lesquels les agents WAPT s'exécutent mettent en œuvre des mécanismes de protection adéquats (confinement, contrôle d'accès, etc.) paramétrés et configurés selon les bonnes pratiques. Les systèmes d'exploitation sont à jour des correctifs en vigueur au moment de l'installation, ils sont sains et exempts de virus, de chevaux de Troie, de modifications de configuration dégradant la sécurité par défaut, etc.	Administrateur système **A5**
H3	Organisationnelle	Il est de la responsabilité de l'Administrateur de s'assurer que les fichiers destinés à être intégrés dans des paquets WAPT proviennent de sources sûres et sont en particulier exempts de virus, chevaux de Troie, etc. Les Administrateurs sont également responsables d'écrire et d'incorporer des scripts setup.py sûrs dans les paquets WAPT.	Administrateurs métier **A3**
H4	Organisationnelle	Un Utilisateur n'a pas les droits d'administration de son poste de travail. Sinon l'Utilisateur est considéré comme un Administrateur Local. En particulier, l'Utilisateur n'a pas les droits d'écriture dans le répertoire d'installation du client WAPT.	Administrateur système **A5**
H5	Organisationnelle	L'Administrateur Local d'un poste client doit être formé à l'exploitation de WAPT, ou à défaut il ne doit pas modifier les fichiers d'installation se trouvant dans le dossier d'installation de WAPT.	RSSI (**A8**)
H6	Organisationnelle	Le serveur sur lequel WAPT est installé est exclusivement dédié à WAPT.	RSSI (**A8**) Administrateur système **A5**

ID	Type de mesure	Description de la mesure	Acteurs en charge de la mesure
H7	Organisationnelle	Les mots de passe utilisés par les Administrateurs sont sensés respecter des critères minimaux de sécurité de l'ANSSI.	**RSSI (A8)**
H8	Organisationnelle	L'environnement sous-jacent est configuré suivant les bonnes pratiques décrites dans le guide de durcissement des postes de travail de l'ANSSI.	**RSSI (A8)** Administrateur système **A5**
H9	Organisationnelle	La machine hébergeant le serveur central se trouve dans une zone sécurisée réputée de confiance. En particulier, le serveur est protégé physiquement en accès et accessible au seul personnel autorisé.	**RSSI (A8)**

4.6. [E_CSPN_ST_17] Menaces

Les agents menaçants à considérer pour l'évaluation de sécurité sont les suivants :

- **Entités non-autorisées** : il s'agit d'un attaquant humain ou d'une entité qui interagit avec WAPT mais qui ne dispose pas d'un accès légitime à celui-ci.
- **Utilisateur final malveillant** : il s'agit d'un utilisateur final ayant accès à un poste sur lequel l'agent WAPT est installé et cherchant à élever ses privilèges sur le poste de travail.

Les Administrateurs métier et les Administrateurs Locaux ne sont pas considérés comme des attaquants.

ID	Description	Interfaces d'attaque	Acteurs de la menace	Biens impactés
M01	**Installation d'un paquet corrompu** Utilisation d'une composante de l'agent WAPT pour déployer un paquet corrompu en contournant la sécurité normalement apportée par la signature du paquet.	**I1, I2, I3, I5, I8**	**A1, A9**	**Tous**
M02	**Altération des valeurs de configuration** Modification ou suppression du paramétrage d'un élément de WAPT défini par un Administrateur légitime de WAPT.	**I8**	**A9**	**(B1) Paquets WAPT**
M03	**Accès illégitime** Récupération des données d'authentification d'un Administrateur, contournement du mécanisme d'authentification de manière à accéder ou altérer un bien sensible stocké sur le serveur.	**I1, I5**	**A1, A9**	**(B1) Paquets WAPT** **(B3) Matériel cryptographique** **(B9) Le système hôte**
M04	**Écoute du réseau** Cette menace correspond à un attaquant qui parviendrait à intercepter et prendre connaissance des communications réseaux entre les agents et le serveur hébergeant WAPT.	**I1, I5**	**A9**	**(B4) Les communications** **(B5) Les données d'inventaire**
M05	**Altération du trafic réseau (Type Man In the Middle)** Cette menace correspond à un attaquant qui parviendrait à modifier les communications réseaux entre les agents et le serveur hébergeant WAPT ou les communications réseau entre la console et le serveur WAPT.	**I1, I5**	**A9**	**(B1) Paquets WAPT** **(B2) Actions déclenchées sur le poste client depuis la console** **(B4) Les communications** **(B5) Les données d'inventaire**
M06	**Altération des journaux** Cette menace correspond à un attaquant qui parviendrait à corrompre les journaux remontant depuis les agents et stockés en base de données.	**I8**	**A1, A9**	**(B6) Les journaux**

ID	Description	Interfaces d'attaque	Acteurs de la menace	Biens impactés
M07	**Récupération du matériel cryptographique** Cette menace correspond à un attaquant qui parviendrait à récupérer ou prendre connaissance des clés cryptographiques.	I3, I8	A1, A9	Tous
M08	**Altération du matériel cryptographique** Cette menace correspond à un attaquant qui viendrait à corrompre de manière illégitime des clés cryptographiques.	I3, I8	A1, A9	(B3) Matériel cryptographique
M09	**Déni de service** Cette menace correspond à un attaquant qui viendrait à affecter la disponibilité des biens sensibles.	I1, I5	A1, A9	(B9) Le système hôte
M10	**Altération ou envoi d'une action non souhaitée sur le poste de travail** Cette menace correspond à un attaquant qui parviendrait à générer ou modifier le flux json contenant des actions et les faire exécuter sur le poste de travail.	I2, I5	A1, A9	(B2) Actions déclenchées sur le poste client depuis la console
M11	**Élévation de privilèges sur le poste de travail** Cette menace correspond à un attaquant qui parviendrait à élever ses privilèges sur le poste de travail, voire même sur l'environnement Active Directory, en utilisant l'environnement WAPT.	I1, I2, I3	A1	(B9) Le système hôte

4.7. [E_CSPN_ST_18] Fonctions évaluées

Note 1 : Cette cible de sécurité inclut uniquement les six fonctions de sécurités décrites dans [E_CSPN_ST_19].

Note 2 : Cette cible de sécurité inclut aucune autre fonction que celles listées dans [E_CSPN_ST_19], conformément à l'exigence [E_CSPN_ST_20].

Tableau 8: Fonctions de sécurité et argumentaire de la couverture des menaces

ID	Description	Argumentaire de couverture des menaces
FS1	**Communications sécurisées**	**M01, M03, M04, M05, M09, M10, M11** Le chiffrement des communications empêche les déploiements non autorisés, la capture des données d'authentification, l'altération des flux.
FS2	**Identification, authentification et contrôle d'accès des utilisateurs**	**M03, M09, M10, M11** L'authentification de l'enregistrement initial d'un agent WAPT empêche l'altération des données d'inventaire. L'authentification des actions locales sur les agents empêche l'installation ou la désinstallation non autorisée de paquets, permet la traçabilité de ces opérations, et prend en charge les autorisation d'accès aux traces. L'authentification des Administrateurs métier sur la console WAPT empêche l'accès non autorisé aux données d'inventaire, le téléversement de paquets non autorisés et les tentatives de lancement d'actions vers les machines clientes.
FS3	**Protection des données, en stockage ou en transit, incluant l'effacement sécurisé**	**M02, M06, M07, M08, M10** Les restrictions d'accès par des mécanismes d'ACL système au matériel cryptographique, traces et inventaires évitent les accès illégitimes et l'altération des données.

ID	Description	Argumentaire de couverture des menaces
FS4	**Fonctions cryptographiques et générateurs de nombres aléatoires**	**M01**, **M03**, **M04**, **M05**, **M08**, **M10**, **M11** La signature des paquets (attributs du fichier *control*, empreintes de fichiers) assure la non altération et l'authenticité des paquets. La signature des actions envoyées aux agents WAPT permet de vérifier la non altération et l'authenticité des actions, et de les autoriser.
FS5	**Autoprotection : démarrage sécurisé, autotests, protection physique, cloisonnement et séparation de domaines.**	**M01**, **M02** La signature des binaires de WAPT avec un certificat issu d'une autorité reconnue par Microsoft permet de s'assurer qu'ils n'ont pas été altérés. La vérification avec une empreinte sha256 des binaires téléchargés depuis le serveur WAPT permet de s'assurer que les données de configuration n'ont pas été altérées.
FS6	**Journalisation**	**M06** Les inventaires et traces des actions et accès sur les machines et le serveur WAPT permettent d'identifier les menaces et de s'assurer de la conformité de la configuration actuelle avec le référentiel de l'organisation.

4.7.1. FS1. Communications sécurisées ✔

4.7.1.1. Communications initiées par l'agent

Les connections https des agents (http 1.1 et websockets) vers le serveur authentifient le serveur au regard de la `CA serveurs https`.

Le serveur https vérifie le certificat client au regard de l'autorité `CA clients https`.

4.7.1.2. Communications initiées par la console

La console télécharge des paquets depuis des dépôts dont elle vérifie que le certificat est issu d'une autorité présente dans son répertoire `%localappdata%/waptconsole/ssl/server`. Les serveurs https des dépôts sont configurés pour n'accepter que les certificats clients issus d'autorités de confiance.

Les requêtes de la console vers le serveur WAPT utilisent le protocole https. La console vérifie que le certificat du serveur est issu de la `CA serveurs https`. Le serveur https vérifie le certificat client au regard de l'autorité `CA clients https`.

4.7.1.3. Connexions websocket des agents

L'accès au serveur WAPT pour l'établissement de la connexion websocket est protégé par une authentification par certificat client.

4.7.1.4. Connexions des agents lors des remontées d'inventaire

Les agents signent leurs données d'inventaire avec leur clé privée, le serveur vérifie la clé et la signature en utilisant le certificat public enregistré dans sa base de données lors de l'enregistrement initial de l'agent.

L'accès au serveur WAPT est protégé par une authentification par certificat client.

4.7.1.5. Connexion des agents pour le téléchargement de paquets

L'accès au(x) dépôt(s) de paquets WAPT est protégé par une authentification par certificat client.

4.7.1.6. Authentification du serveur par les agents

Lorsque l'agent se connecte au serveur par des requêtes HTTPS, il vérifie que le certificat du serveur est valide et qu'il provient d'une autorité de certification de confiance. À l'installation de l'agent, on épingle de certificat qui permettra d'authentifier le serveur.

4.7.1.7. Authentification du(des) dépôt(s) par les agents

Lorsque l'agent se connecte à un dépôt par des requêtes HTTPS, il vérifie que le certificat du dépôt est valide et qu'il provient d'une autorité de certification de confiance. À l'installation de l'agent, on épingle de certificat qui permettra d'authentifier le serveur.

4.7.2. FS2. Identification, authentification et contrôle d'accès des utilisateurs ✔

4.7.2.1. Enregistrement initial d'un agent WAPT

Pour exister dans la base de données et ainsi apparaître dans la console WAPT, une machine doit s'enregistrer auprès du serveur WAPT avec une commande `register`.

L'action `register` est exécutée automatiquement lors de l'installation ou de la mise à jour de l'agent WAPT si la machine est correctement enregistrée avec un compte machine *Kerberos* dans le domaine *Active Directory* de l'Organisation.

Si la machine ne présente pas au serveur WAPT un ticket K*erberos* valide, alors l'action `register` échoue avant de nécessiter un accès à la base de données.

Lors de l'enregistrement, le poste client génère une paire de clés RSA dans le répertoire privé local et envoie au serveur une demande de signature de certificat avec le ticket K*erberos*.

Si le ticket Kerberos est valide, le Serveur WAPT enregistre l'agent WAPT dans sa base de données, signe le *CSR* (Certificate Signing Request), stocke le certificat dans sa base de données et renvoie le certificat signé à l'agent WAPT.

Si un agent WAPT est déjà enregistré, il peut se ré-enregistrer sans ticket kerberos en utilisant le certificat signé de son serveur actuel.

Si l'authentification *Kerberos* échoue ou n'est pas disponible, le serveur *Nginx* envoie un statut non autorisé, et le client demande à l'Administrateur Local d'entrer les informations d'identification d'un compte du serveur WAPT ayant le privilège *admin* ou le privilège *register_host*. Ce compte est défini sur le serveur WAPT localement, ou authentifié par un annuaire *LDAP / Active Directory*.

Note : La méthode avec Kerberos assume que le serveur Active Directory répond au moment de l'enregistrement.

4.7.2.2. Actions locales sur les agents

L'Utilisateur du poste de travail peut interagir avec l'agent WAPT par des actions HTTPS locales. L'Utilisateur est identifié par son nom d'utilisateur ce qui détermine les propriétés de sa session locale.

Les actions de l'Utilisateur (installations, désinstallations, mises à jour de paquets) sont authentifiées par le service local en utilisant un jeton chiffré stocké dans un fichier dans le répertoire personnel associé à la session de l'Utilisateur. Les *ACLs* du fichier jeton sont ajustées pour ne permettre sa lecture que par l'utilisateur (mécanisme « *filetoken* »)

L'accès aux actions est conditionné par l'appartenance du compte de l'Utilisateur à des groupes de sécurité du système local du poste (cf. règles self-service définies par un paquet de type *self-service*).

4.7.2.3. Authentification des Administrateurs métier sur la console WAPT

La connexion HTTPS de la console d'administration sur le serveur est d'abord authentifiée par le certificat client de l'Administrateur métier.

La requête de login initiale est authentifiée par le ticket de session *kerberos* de l'Administrateur métier. Elle permet de récupérer un jeton de session qui authentifiera les requêtes qui suivront.

Les *ACLs* WAPT associées au compte de l'Administrateur métier déterminent les fonctions accessibles du serveur. Elles permettent de faciliter l'organisation et ne sont pas considérées comme un élément de sécurité.

Le serveur maintient en mémoire une liste des sessions actives grâce à un mécanisme clé-valeur opéré par le service « *waptserver* ». Cela permet de retrouver pour chaque session les *ACLs* associées à l'utilisateur. Pour cela, le port 11212 est ouvert sur l'interface *loopback* du serveur et permet aux process locaux *waptserver* de vérifier l'existence de la session et des permissions associées.

4.7.3. FS3. Protection des données, en stockage ou en transit, incluant l'effacement sécurisé ✔

4.7.3.1. Accès au répertoire d'installation de l'agent WAPT

Le répertoire d'installation `<wapt>` (`C:\Program Files (x86)\wapt` par défaut) est accessible en lecture et modification :

- aux Administrateurs Locaux à travers un accès local au répertoire d'installation de l'agent WAPT ;
- aux Administrateurs métier à travers le mécanisme de déploiement des mises à jour de l'agent WAPT.

Les Utilisateurs n'ont pas d'accès en écriture au répertoire d'installation de l'agent WAPT.

Les restrictions d'accès au dossier `<wapt>` reposent sur le mécanisme *ACL* standard du système d'exploitation et sont appliquées pendant l'installation de l'agent WAPT.

Une base de données avec les informations limitées aux besoins des fonctions s'exécutant avec les droits des utilisateurs (*session-setup* en particulier).

4.7.3.2. Accès au répertoire de stockage <wapt>/private

Le répertoire `<wapt>/private` (`C:\Program Files (x86)\wapt\private` par défaut) contient :

- Le couple clé privé / certificat identifiant l'agent auprès du serveur.
- La base de données de l'état de l'agent, de l'état des paquets et des données d'audits.
- Les données persistantes des paquets dans le sous-répertoire `<wapt>/private/persistent`.

Aucun droit d'accès au répertoire n'est accordé à aucun Utilisateur, quel qu'il soit. Seul l'agent WAPT et les Administrateurs Locaux ont accès en lecture et écriture à ce répertoire.

Les restrictions d'accès au dossier `<wapt>/private` reposent sur le mécanisme d'*ACL* standard du système d'exploitation et sont appliquées pendant l'installation de l'agent WAPT.

4.7.3.3. Accès au couple clé privée / certificat de l'Administrateur métier

La clé privée doit être stockée par l'Administrateur métier dans un dossier qu'il est seul à pouvoir parcourir et qu'il estime sûr. Lors de la génération des clés par la console, il est proposé de les stocker dans le répertoire personnel de l'Administrateur métier dans un dossier `private` de son répertoire personnel.

La clé est chiffrée par une clé dérivée d'un mot de passe fort fourni par l'Administrateur métier.

4.7.4. FS4. Fonctions cryptographiques et générateurs de nombres aléatoires ✔

4.7.4.1. Signature des attributs du fichier *control*

Les métadonnées d'un paquet (attributs) sont définies dans un fichier texte du paquet nommé `control`.

Une somme de contrôle de l'ensemble des attributs du fichier `control` est générée, puis elle est signée par la clé privée du Développeur du paquet. La signature est ajoutée au fichier `control`.

Lors de la mise à jour des paquets disponibles, l'agent est ainsi en mesure de contrôler que le certificat du Développeur du paquet est issu d'une autorité présente dans son répertoire local `<wapt>/ssl`.

La clé publique permet de vérifier la signature des attributs du paquet et de l'authentifier.

La signature de la somme de contrôle permet de vérifier l'intégrité du fichier `control`.

4.7.4.2. Signature des paquets WAPT

Les paquets sont une archive ZIP. Lors de la signature du paquet, on génère un fichier `manifest` contenant la liste des fichiers de l'archive avec la somme de contrôle de chaque fichier.

La somme de contrôle de ce fichier `manifest` est signée par la clé privée du Développeur du paquet.

L'agent est ainsi en mesure de contrôler que le certificat du Développeur du paquet est issu d'une autorité présente dans son répertoire local `<wapt>/ssl`.

La clé publique permet de vérifier la signature du fichier `manifest` et d'authentifier le paquet. La liste des fichiers et les sommes de contrôle du fichier `manifest` permettent de vérifier l'intégrité des fichiers constituant le paquet WAPT.

4.7.4.3. Signature des actions envoyées aux agents WAPT

Une action est définie par un ensemble de propriétés encodées en JSON par la console WAPT.

Une somme de contrôle des données JSON est générée, puis signée par la clé privée de l'Administrateur. La signature est ajoutée aux données JSON.

Lors de la réception de l'action, l'agent est ainsi en mesure de contrôler que le certificat qui a signé l'action est issu d'une

autorité présente dans son répertoire local `<wapt>/ssl`.

La clé publique permet de vérifier la signature de l'action et de l'authentifier.

La signature de la somme de contrôle permet de vérifier l'intégrité de l'action.

4.7.5. FS5. Autoprotection : démarrage sécurisé, autotests, protection physique, cloisonnement et séparation de domaines ✔

L'ensemble des binaires diffusés par WAPT : l'installeur et les binaires inclus sont signés par Tranquil IT, avec un certificat EV Code-Signing issu d'une autorité reconnue par Microsoft.

Lors de la mise à jour de l'agent, « waptdeploy » vérifie que l'empreinte de l'installeur téléchargé correspond bien avec celle fournie en argument (argument `--hash`). L'argument `--hash` est stocké dans une GPO donc n'est modifiable que par un administrateur de l'organisation.

Un utilisateur ne peut pas désinstaller à travers le self-service un paquet WAPT imposé par un Administrateur Métier et déployé par un paquet Machine, un paquet Unité Organisationnelle ou un paquet Groupe AD.

4.7.6. FS6. Journalisation ✔

Les processus des agents, du serveur WAPT et du serveur https *Nginx* génèrent des traces de leur fonctionnement respectif dans des fichiers textes protégés en lecture et écriture par les *ACL* du système de fichiers. La console d'administration WAPT ne journalise rien par elle-même, elle ne fait que requêter le serveur WAPT.

Le dernier état de chaque paquet installé est stocké dans une base locale de l'agent protégé en écriture par les *ACLs* du système de fichiers. Ces données sont envoyées au serveur WAPT et stockées dans une base de données PostgreSQL dont l'accès est restreint au seul compte propriétaire du process serveur WAPT.

Lorsque l'agent envoie ses journaux au serveur WAPT, il les signe avec sa clé privée. Le process serveur vérifie l'authenticité et l'intégrité de ces données grâce au certificat / clé publique de l'agent stocké dans la base de données du serveur.

La console d'administration permet de consulter ces informations. Il faut néanmoins disposer du rôle *admin* ou *view* sur le serveur pour y avoir accès.

4.8. [E_CSPN_ST_21] Surface d'attaque du produit

Tableau 9: Types de surface d'attaque

Type de surface d'attaque		Interfaces (accessibles ou non accessibles)	Fonction concernée (évaluée ou non évaluée)	Acteurs ayant accès aux interfaces
Interfaces logiques des Machines administrées	**I1**	Port TCP 127.0.0.1:8088 ouvert par le service WAPT	Service résident WAPT (évalué 4.7.2.2 Actions locales sur les agents)	**A1**, **A5**
	I2	Actions websocket	Pilotage du service WAPT des machines administrées depuis la console WAPT (évalué 4.7.4.3 Signature des actions envoyées aux agents WAPT)	**A1**, **A2**, **A3**, **A4**
	I3	Script setup.py des paquets	Installation, Audit, Suppression de configurations et logiciels, configuration session utilisateur (**non évalué**) **A1**, **A2**, **A3**, **A4**	**A1**, **A2**, **A3**, **A4**
Interfaces logiques du serveur WAPT	**I4**	Port TCP 127.0.0.1:5432 du serveur Postgresql	Stockage des données d'inventaire (**non évalué**)	**A5**
	I5	Port TCP 0.0.0.0:443 nginx	Mise à disposition des paquets Tunnel websocket pour les actions distantes Remontée d'inventaire et d'état des machines Accès à l'inventaire des machines. (évalués, 4.7.1 FS1. Communications sécurisées ✔ et 4.7.2 FS2. Identification, authentification et contrôle d'accès des utilisateurs ✔)	**A1**, **A2**, **A3**, **A4**, **A5**, **A9**
	I6	webservice waptserver (Port TCP 127.0.0.1:8080)	Tunnel websocket pour piloter les agents WAPT Accès à l'inventaire des agents WAPT Remontée inventaire des agents WAPT (**communication intra-serveur nginx <> waptserver**) (évalués, 4.7.1 FS1. Communications sécurisées ✔, 4.7.2 FS2. Identification, authentification et contrôle d'accès des utilisateurs ✔ et 4.7.4.3 Signature des actions envoyées aux agents WAPT)	**A1**, **A5**
	I7	webservice waptserver (Port TCP 127.0.0.1:11212)	Memcache (**communication intra-serveur waptserver <> waptserver**, évalué 4.7.2.3 Authentification des Administrateurs métier sur la console WAPT)	**A5**
	I8	Port TCP 0.0.0.0:22 ssh	Administration du serveur WAPT (**non évalué**)	**A5**, **A9**

4.9. [E_CSPN_ST_22] Interfaces non documentée

Néant

4.10. [E_CSPN_ST_23] Fonctions désactivées

Les fonctions listées ci-dessous nécessitent une configuration pour fonctionner. Une documentation spécifique est disponible pour que ces fonctions ne soient pas mises en œuvre. Ces fonctions sont :

- WADS (déploiement initial de postes, équivalent Microsoft MDT).
- WAPT Windows Updates (équivalent Microsoft WSUS).

- Le *peercache*.
- Les dépôts secondaires.

L'évaluation devra confirmer qu'elles ne sont pas ré-activables par un attaquant.

4.11. [E_CSPN_ST_24] Fonctions non évaluées

Les fonctions listées ci-dessous sont actives dans la version du produit livrée à l'évaluation :

- Les restrictions fonctionnelles liées aux *ACLs* dans WAPT (l'évaluation se fait avec un compte qui a l'*ACL admin*, c'est à dire qui dispose de tous les droits). Cet élément est essentiellement organisationnel.

Fin du document