Cible de sécurité CSPN

Produit WAPT-Enterprise version 1.5.0.13-amo

Catégorie « Administration et supervision de la sécurité »

Référence : *CSPN-ST-WAPT-1.0.6*

Date : le 8/12/2017

Code interne : TIS001

AMOSSYS SAS	**TRANQUIL IT SYSTEMS SAS**
Siège : 4 bis allée du Bâtiment ● 35000 Rennes	**Siège**:12 avenue Jules Verne●44230 Saint Sébastien s/Loire
RCS : Rennes B 493 348 890	**RCS** : Nantes B 443 884 580
www.amossys.fr	*www.tranquil.it*

FICHE D'EVOLUTIONS

Révision	Date	Description	Rédacteur(s)
1.00	17/02/2017	Création du document	Alexandre DELOUP Antoine COUTANT
1.01-travail	27/02/2017	Précisions	Hubert TOUVET
1.02-travail	08/03/2017	Partagé avec l'ANSSI	Hervé GUERIN
1.03-travail	28/04/2017	Prise en compte des premières remarques de l'ANSSI	Hubert TOUVET Hervé GUERIN
1.04	15/05/2017	Version jointe au dossier de demande de qualification	Hubert TOUVET Antoine COUTANT
1.05	08/06/2017	Prise en compte des remarques de l'audit à blanc	Denis CARDON
1.06	8/12/2017	Prise en compte des remarques du bilan du premier audit CSPN	Denis CARDON Hubert TOUVET Hervé GUERIN

Ce document a été validé par Tranquil IT Systems.

Sommaire

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN[1] promu par l'ANSSI[2], du produit « WAPT » développé par la société **Tranquil IT Systems**.

La TOE[3] considérée est la solution complète WAPT (serveur + agents).

1.2. IDENTIFICATION DU PRODUIT

Éditeur	**Tranquil IT Systems** 12, avenue Jules Verne 44230 SAINT SEBASTIEN SUR LOIRE
Lien vers l'organisation	https://www.tranquil.it/
Nom commercial du produit	WAPT
Numéro de la version évaluée	1.5.0.13-amo
Catégorie du produit	Administration et supervision de la sécurité

1.3. REFERENCES

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

- https://www.wapt.fr/ : site officiel du produit ;
- https://www.wapt.fr/fr/doc/ : documentation officielle du produit ;
- https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_MDP_NoteTech.pdf : Recommandations de sécurité relatives aux mots de passe ;
- https://wapt.fr/fr/1.5.0.13-amo/ : Documentation en ligne de WAPT pour la version évaluée.

[1] Certification de Sécurité de Premier Niveau

[2] Agence nationale de la sécurité des systèmes d'information

[3] *Target Of Evaluation*

2. DESCRIPTION DU PRODUIT

2.1. DESCRIPTION GENERALE

WAPT automatise l'installation, la (post)configuration, la mise à jour et la suppression de logiciels sur un parc Windows. 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 son nom.

WAPT est constitué de trois sous-ensembles tels que décrits ci-après.

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 :

- un ou plusieurs *waptserver* qui stockent de manière centralisée l'inventaire du parc. En complément, ils servent à notifier les agents WAPT d'opérations immédiates ;
- un ou plusieurs *waptrepo* qui stockent les paquets WAPT, les paquets groupe et les paquets machine.

2.1.2. Composante client

La composante client est elle-même découpée en une sous-composante obligatoire et trois sous-composantes optionnelles :

- un agent *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 ;
- un service *waptservice* optionnel 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 une page web à l'adresse http://localhost:8088 qui permet à des utilisateurs autorisés d'installer ou de supprimer des logiciels sur leur poste de travail ;
- un service *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 ;
- un service *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.

2.1.3. Composante console

La console d'administration *waptconsole* est installée sur un poste client. Elle fournit à l'administrateur ou au gestionnaire de déploiement 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 ou du gestionnaire de déploiement pourront être installés sur les postes clients équipés de leur clé publique. La console permet d'importer des paquets depuis des dépôts tiers ; l'administrateur valide et signe avec sa clé privée le paquet WAPT récupéré avant de le pousser vers son dépôt privé.

L'installateur de l'agent WAPT est généré par l'administrateur 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 sont déployés sur le parc manuellement ou de manière automatisée (ex : GPO). 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.

Le produit est disponible en deux versions :

- *WAPT Server* qui permet la gestion d'un parc de postes Windows. Il intègre un serveur web qui fait office de dépôt et un serveur d'inventaire pour le suivi des déploiements et la configuration des machines ;
- *WAPT Starter* qui permet à des particuliers ou des TPE de bénéficier de WAPT en s'appuyant sur les dépôts de Tranquil IT Systems ;

Seule la version *WAPT Server* sera évaluée.

2.2. PRINCIPE DE FONCTIONNEMENT

L'installateur de WAPT Server est téléchargeable à l'adresse suivante :

http://wapt.tranquil.it/wapt/releases/latest/

L'administrateur 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'installateur 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 peut ensuite être installé directement sur les postes par la méthode choisie par les administrateurs locaux des machines (déploiement par GPO, installation manuelle, etc.).

WAPT peut s'utiliser sur les machines du parc en ligne de commande (ex : wapt-get install tis-firefox), via l'interface graphique *waptconsole* ou au travers de l'interface Web locale de gestion (http://localhost:8088/).

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>* (respectivement *wapt-get remove <nom du paquet>*) permet d'installer (respectivement désinstaller) un logiciel.

La page d'accueil de la console Web locale des agents donne diverses informations sur la version de WAPT installée. L'onglet « Paquets installés » donne la liste des paquets disponibles sur le(s) dépôt(s) configuré(s). À partir de cet onglet, il est possible d'installer/de désinstaller des paquets

donnés. L'onglet « Tâches » permet de suivre les tâches en cours, en erreur, ou effectuées par WAPT. En particulier, il est possible, à tout moment, d'interrompre une tâche en cours.

La console Web permet uniquement de gérer la machine locale, sans impact sur le serveur WAPT ou les autres postes gérés par la solution.

Le processus d'installation est entièrement décrit dans la documentation disponible en ligne, et la société Tranquil IT Systems propose en complément des formations et prestations standards ou sur-mesure pour aider les utilisateurs et administrateurs de WAPT à prendre en main et utiliser WAPT.

2.3. DESCRIPTION DES DEPENDANCES

L'installateur de l'agent WAPT emporte 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.

2.4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

WAPT est destiné aux gestionnaires de parcs de PC, de portables et de serveurs fonctionnant sous Windows.

Le serveur peut être installé sous Debian Linux, CentOS (avec et sans SELinux) ou Windows et Windows Serveur, et les agents et la console d'administration (c'est-à-dire la partie cliente) ne sont disponibles que sur les systèmes Windows (voir la liste exhaustive des versions dans la documentation WAPT).

Cependant seules les versions suivantes sont supportées dans le cadre de la version sécurisée (candidate pour la certification CSPN) :

- Pour la partie serveur : Linux CentOS avec SELinux,
- Pour la partie agents et la console d'administration : Windows 7, Windows 10 et Windows server 2008 R2.

2.5. PERIMETRE DE L'EVALUATION

2.5.1. Périmètre

L'évaluation porte sur :

- Le *serveur WAPT* (serveur « core » et dépôt de paquets) ;
- Les *agents WAPT* ;
- La console de management ;
- Les communications réseaux entre ces différentes composantes.

Le téléchargement des mises à jour des logiciels, la rédaction en python du script WAPT ainsi que la fourniture de tous les autres fichiers servant à constituer le paquet WAPT, de même que la gestion des clés privées de signature des paquets et la gestion et la révocation des certificats SSL, ne font pas partie de la TOE.

2.5.2. Plateforme d'évaluation

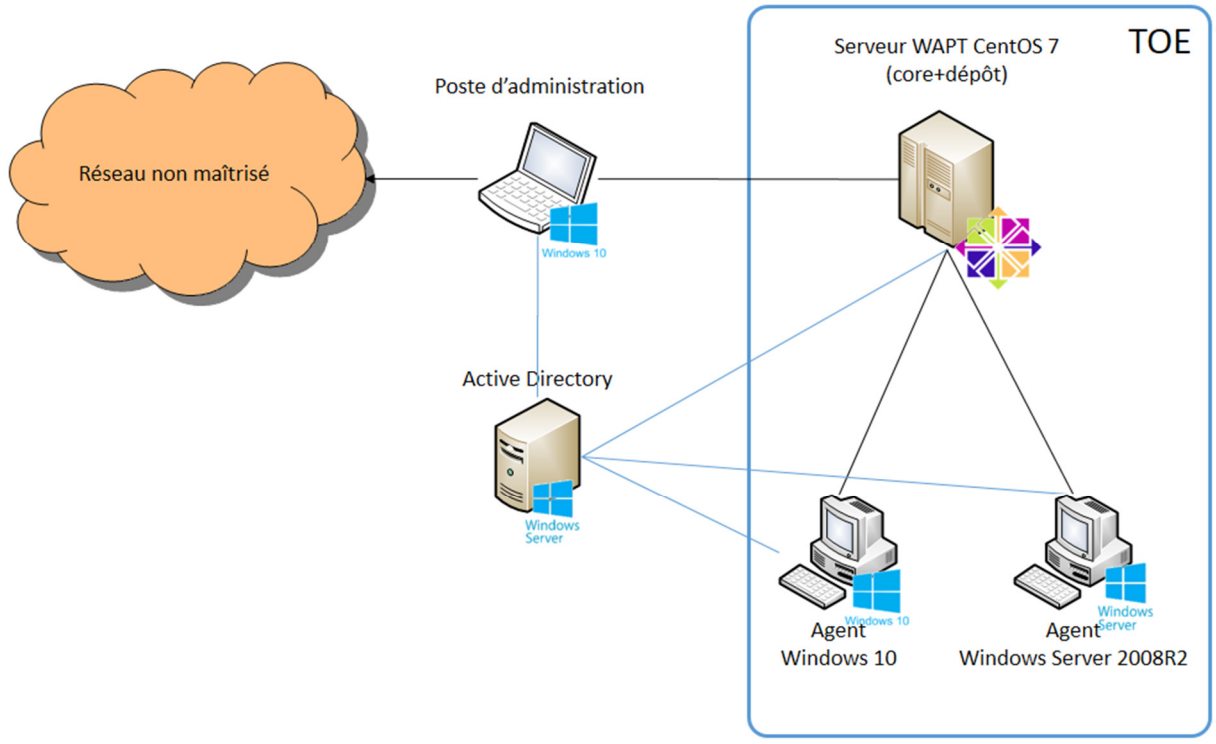
L'évaluation portera sur :

- Le serveur WAPT (serveur « core » et dépôt de paquets) installé sur CentOS 7 avec SELinux ;
- Les agents WAPT installés sur Windows 10, Windows 7 et Windows Server 2008R2, y compris la console de management.

Un poste d'administration (*waptconsole*) est connecté au serveur WAPT au travers d'un réseau local. Ce poste 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 souhaite intégrer à son dépôt WAPT privé.

Tous les postes sont connectés à un serveur Active Directory permettant l'authentification des postes et des utilisateurs.

Illustration 1 : Plateforme d'évaluation



3. PROBLEMATIQUE DE SECURITE

3.1. DESCRIPTION DES UTILISATEURS TYPIQUES

Par définition, les utilisateurs sont les personnes et services applicatifs qui interagissent avec le produit évalué.

Les rôles suivants doivent être pris en considération dans le cadre de l'évaluation de sécurité :

- ***Utilisateur :*** individu/utilisateur d'une machine équipée de l'agent WAPT ;
- ***Gestionnaire de déploiement :*** individu pouvant signer des paquets ne contenant pas de code python (en général les paquets de type « groupe » et « machine ») et les télécharger sur le dépôt principal ;
- ***Administrateur :*** individu pouvant signer des paquets (qu'ils intègrent ou non du code python) et les télécharger sur le dépôt principal. L'administrateur dispose des droits pour packager et signer une application sur la TOE ;
- ***Administrateur local*** : utilisateur disposant des droits d'administration locale sur les postes.

3.2. DESCRIPTION DES BIENS SENSIBLES

Par définition, un bien sensible est une donnée (ou fonction) jugée comme ayant de la valeur par la TOE. Sa valeur est estimée selon des critères de sécurité (aussi appelés besoins de sécurité) : disponibilité, intégrité, confidentialité et authenticité.

Les biens à protéger sont les suivants :

- **B1.COMMUNICATIONS**

  Communications entre le serveur central et les agents ainsi que communications entre la console Waptconsole et le serveur.

  Besoin de sécurité : intégrité, confidentialité et authenticité.

- **B2.DONNEES INVENTAIRE**

  Informations sur l'état de déploiement des paquets, ainsi que configuration matérielle et logicielle des postes clients.

  Besoin de sécurité : intégrité et confidentialité

- **B3.JOURNAUX**

  Journaux générés par la solution (sur le serveur central et les agents).

  Besoin de sécurité : disponibilité.

- **B4.CONFIGURATION**

  Paramètres de configuration du serveur (clés du serveur https, configuration accès à la base de données, configuration de l'authentification et autorisation au serveur).

  Besoin de sécurité : intégrité et confidentialité.

- **B5.POSTES CLIENTS**

  Postes clients managés par WAPT (contenu du répertoire WAPT incluant les binaires, les dll, les fichiers de configuration et la base de données).

  Besoin de sécurité : intégrité.

- **B6.AUTHENTIFICATION**

  Données d'authentification à la console d'administration du serveur ainsi que les données d'authentification des agents sur le serveur (clé publique de chaque agent WAPT).

  Besoin de sécurité : intégrité et confidentialité.

3.3. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Par définition, les hypothèses sont des déclarations portant sur le contexte d'emploi de la TOE ou de son environnement.

Les hypothèses suivantes sur l'environnement de la TOE doivent être considérées :

- **H1.ADMINISTRATEURS ET GESTIONNAIRES DE DEPLOIEMENT**

  Les administrateurs et gestionnaires de déploiement respectent les règles de l'art en matière de sécurité dans leur domaine, en particulier dès lors qu'il s'agit d'un poste de travail, et ils sont formés à l'utilisation de la TOE. En particulier, ils doivent s'assurer que leurs identifiants et clés de sécurité restent secrets et que leurs mots de passe respectent les recommandations de l'ANSSI (voir le document cité au chapitre 1.3 Références).

- **H2.SYSTÈME SAIN**

  Les systèmes d'exploitation support de la TOE mettent en œuvre des mécanismes de protection adéquats (confinement, contrôle d'accès, etc.) paramétrés et configurés selon les bonnes pratiques. De plus, le système d'exploitation support de la TOE est à jour des correctifs en vigueur au moment de l'installation, sain et exempt de virus, chevaux de Troie, etc.

- **H3.INTÉGRITÉ TOE**

  Toutes les bibliothèques et les outils nécessaires à l'installation et à la configuration du produit sont intègres.

- **H4.INTÉGRITÉ PAQUETS**

  Il est de la responsabilité de l'administrateur de s'assurer que les fichiers destinés à être intégrés dans les paquets WAPT proviennent de sources sûres et sont en particuliers exempts de virus, chevaux de Troie, etc.

- **H5.UTILISATEURS DES POSTES CLIENTS**

  Un utilisateur n'a pas les droits d'administration de son poste de travail. Sinon il est considéré comme relevant de la catégorie « Administrateurs des postes clients ». En particulier, il n'a pas les droits d'écriture dans le répertoire d'installation du client WAPT.

- **H6.ADMINISTRATEURS DES POSTES CLIENTS**

  L'administrateur d'un poste client doit être formé à la TOE, ou ne pas modifier les fichiers d'installation se trouvant dans le dossier d'installation de WAPT.

3.4. DESCRIPTION DES MENACES

Par définition, une menace est une action ou un événement susceptible de porter préjudice à la sécurité de la cible évaluée.

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

- **Entités non autorisées** : un attaquant humain ou entité qui interagit avec la TOE mais ne dispose pas d'un accès légitime à celle-ci.

Les administrateurs et les gestionnaires de déploiement ne sont pas considérés comme des attaquants.

Les menaces qui portent sur les biens sensibles de la TOE sont les suivantes :

- **M1.INSTALLATION LOGICIEL MALVEILLANT**

  Un attaquant parvient à utiliser une composante de l'agent WAPT pour installer une application malveillante de façon pérenne, ou désinstaller ou désactiver une composante de sécurité du poste sur lequel l'agent WAPT est installé.

- **M2.ALTÉRATION CONFIGURATION**

  Le dysfonctionnement de la TOE ou l'attaque d'une entité malveillante entraîne la modification ou la suppression du paramétrage d'un élément de la TOE défini par l'administrateur de la solution.

- **M3.ACCÈS ILLÉGITIME**

  Un attaquant parvient à récupérer les données d'authentification d'un administrateur, à contourner le mécanisme d'authentification, et à accéder ou altérer les biens sensibles stockés sur le serveur ou un attaquant parvient à se faire passer pour un agent WAPT.

- **M4.ÉCOUTE RÉSEAU**

  Un attaquant parvient à intercepter et prendre connaissance des communications réseaux entre les agents et le serveur hébergeant WAPT.

- **M5.ALTÉRATION RÉSEAU (TYPE « MAN IN THE MIDDLE »)**

  Un attaquant parvient à modifier les communications réseaux entre les agents et le serveur hébergeant WAPT.

3.5. DESCRIPTION DES FONCTIONS DE SECURITE

Par définition, les fonctions de sécurité sont l'ensemble des mesures techniques et mécanismes mis en œuvre dans la TOE pour protéger de façon proportionnée les biens sensibles de la TOE contre les menaces identifiées.

Les fonctions de sécurité essentielles de la TOE sont les suivantes :

- **F1.AUTHENTIFICATION CONTRÔLE ACCÈS**

  Le serveur WAPT opère une authentification et un contrôle d'accès aux données d'inventaire stockées sur le serveur WAPT, à l'ajout ou suppression de paquets sur le dépôt par son intermédiaire ainsi qu'une authentification des agents WAPT.

- **F2.PROTECTION DONNÉES**

  L'agent WAPT protège l'intégrité du processus d'installation des logiciels installés par son intermédiaire.

- **F3.COMMUNICATIONS SÉCURISÉES**

  Les communications entre les agents et le serveur et entre la console et le serveur sont protégées en confidentialité, intégrité et authenticité.

- **F4.SIGNATURE PAQUETS**

  Les paquets installables au travers de l'agent WAPT sont signés par la clé privée d'un administrateur (tous types de paquets) ou celle d'un gestionnaire de déploiement (paquet ne contenant pas de code python).

3.6. MATRICES DE COUVERTURES

3.6.1. Menaces et biens sensibles

La matrice suivante présente la couverture des menaces sur les biens sensibles (les lettres "D", "I", "C" et "A" représentent respectivement les besoins de Disponibilité, Intégrité, Confidentialité et Authenticité) :

	B1.COMMUNICATIONS	B2.DONNEES INVENTAIRE	B3.JOURNAUX	B4.CONFIGURATION	B5.POSTES-CLIENTS	B6.AUTHENTIFICATION
M1.INSTALLATION LOGICIEL MALVEILLANT	IC				I	
M2.ALTÉRATION CONFIGURATION				I		
M3.ACCÈS ILLÉGITIME		IC	D	IC	I	IC
M4.ÉCOUTE RÉSEAU	C	C				
M5.ALTÉRATION RÉSEAU	IA	IA				

Tableau 1 - Couverture des biens sensibles par les menaces

3.6.2. Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

	F1.AUTHENTIFICATION CONTRÔLE ACCÈS	F2.PROTECTION DONNÉES	F3.COMMUNICATIONS SÉCURISÉES	F4.SIGNATURE PAQUETS
M1.INSTALLATION LOGICIEL MALVEILLANT	√	√		√
M2.ALTÉRATION CONFIGURATION	√	√		
M3.ACCÈS ILLÉGITIME	√			
M4.ÉCOUTE RÉSEAU			√	
M5.ALTÉRATION RÉSEAU			√	√

Tableau 2 - Couverture des menaces par les fonctions de sécurité

Fin du document