Cible de sécurité CSPN – SCOOP-MS			
Auteur :	Arnaud TARRAGO, Pascal SITBON, Pierre NGUYEN	***Visa :***	
Référence :	**CR-I2D-2012-047-1c**	***Date :***	29/10/2012

0. OBJECTIF DU DOCUMENT

Ce document présente la cible de sécurité CSPN du dispositif SCOOP-MS (*Selective COntrol Of Peripheral, version MassStorage)*. Il respecte le formalisme et les rubriques classiques des cibles de sécurité CSPN.

1. IDENTIFICATION DU PRODUIT

Organisation éditrice	SECLAB-FR
Lien vers l'organisation	http://www.seclab.fr
Nom commercial du produit	SCOOP-MS
Numéro de la version évaluée	1.0
Catégorie de produit	Anti-virus, protection contre les codes malicieux

2. ARGUMENTAIRE (DESCRIPTION) DU PRODUIT

2.1. DESCRIPTION GENERALE DU PRODUIT

Le produit est un dispositif de filtrage permettant un transfert unidirectionnel de données entre un dispositif de stockage de masse (par exemple une clef USB) situé en zone basse et une machine haute. Il permet le passage d'information du dispositif de stockage vers la machine haute via un point de stockage relais, avec des restrictions sur le contenu des données échangées. La transmission des informations reste à l'initiative de la zone haute. **La zone haute correspond au niveau de confiance le plus élevé**. Le dispositif de stockage contient **potentiellement du code permettant de commettre des malveillances**

à l'insu de son utilisateur. On considère que le dispositif SCOOP-MS est le seul point d'entrée entre la zone basse et la zone haute.

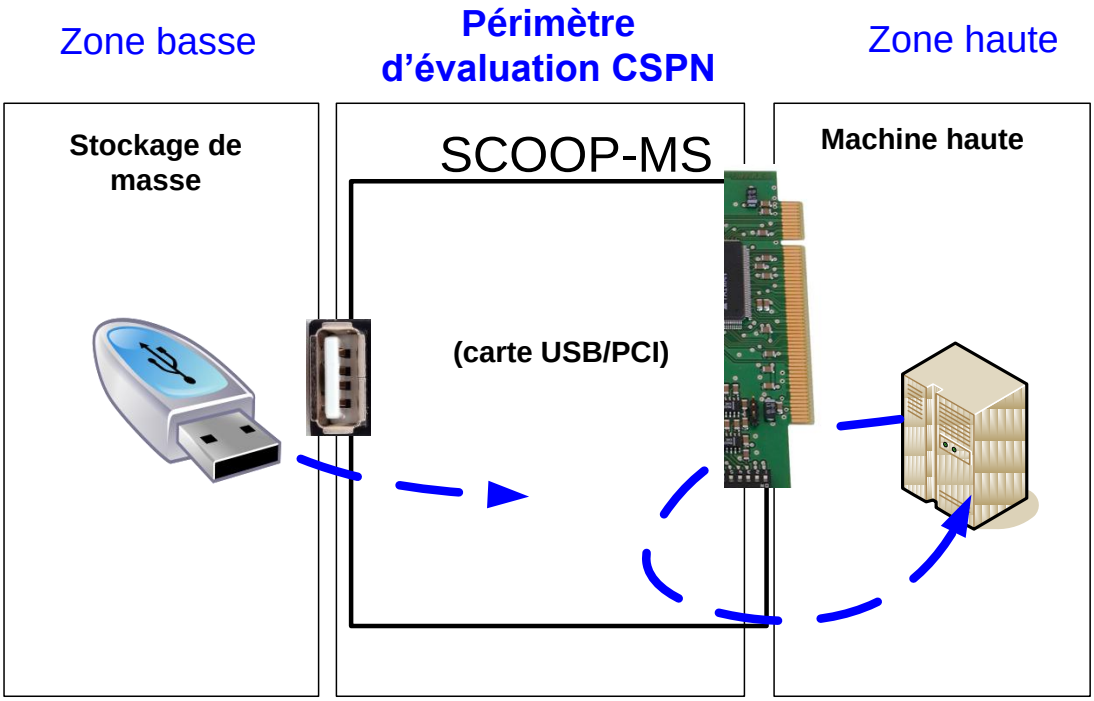

Figure 1. Fonctionnement général du produit et périmètre d'évaluation CSPN

2.2. DESCRIPTION DE LA MANIERE D'UTILISER LE PRODUIT

L'utilisateur se présente devant la connexion USB du dispositif avec son périphérique de stockage de masse USB contenant les fichiers à transférer. Lorsqu'il branche son périphérique, les fichiers de la racine du périphérique sont recopiés dans le répertoire « SCOOP-MS » du dispositif. Une LED indique à l'utilisateur lorsque la copie est terminée afin qu'il puisse retirer son périphérique. En parallèle, le nom de la clef change sur le poste haut (dans l'explorateur windows, sur le bureau, …): la clef se nomme « SC-COPYING » durant le transfert et « SC-READY » quand le transfert est terminé.

La figure 2 illustre le cas d'usage de la remontée d'informations en provenance de capteurs sans fil (zone basse) vers une salle de supervision (zone haute).

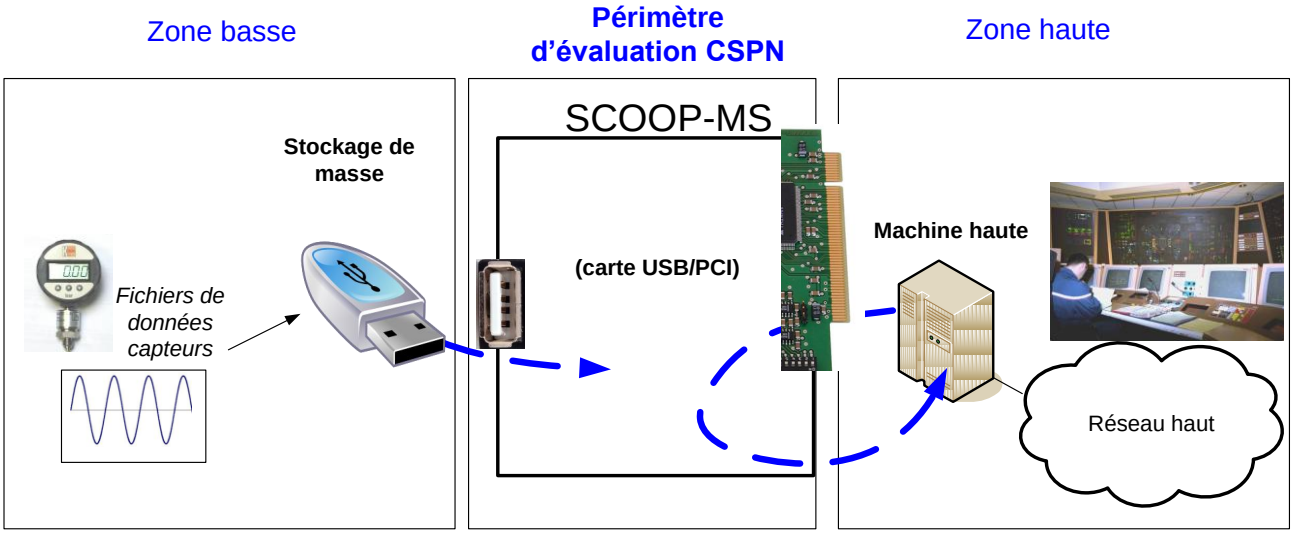

Figure 2. Cas d'usage du produit

2.3. DESCRIPTION DE L'ENVIRONNEMENT PREVU POUR SON UTILISATION

L'environnement est considéré comme physiquement sûr au niveau du produit et de la machine haute. Ainsi, le produit ne prend pas en compte des mesures de sécurité particulières au niveau de la malveillance matérielle et/ou utilisant un accès physique au produit.

L'utilisation concerne uniquement des transferts de fichiers au format texte, ne comportant que des caractères ayant un code ASCII défini dans des intervalles déterminés (décrits dans la documentation utilisateur), avec une longueur de ligne limitée à un nombre maximum de caractères.

De la même façon, un contrôle des caractères utilisés pour nommer le fichier est effectué avec des règles similaires.

Ces fichiers, de type « texte », ont aussi une taille limitée et ne peuvent pas utiliser n'importe quelle extension. Le **contenu de ces fichiers n'est pas confidentiel**.

2.4. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Les attaques nécessitant un accès physique au produit ne sont pas prises en compte par hypothèse (cf. §2.3).

[H.SEC_PHYSIQUE] Le dispositif SCOOP-MS doit être utilisé dans un environnement considéré comme physiquement sûr (la carte PCI est mise dans une machine appartenant à la zone haute) au niveau du produit et de la machine haute. Ainsi, le produit ne prend pas en compte des mesures de sécurité particulières au niveau de malveillances matérielles et/ou utilisant un accès physique au produit.

[H.INIT] Le dispositif SCOOP-MS est entièrement configuré lors de sa fabrication, donc avant sa livraison. Les fonctions du produit sont figées et ne sont plus modifiables par la suite. La seule action de l'administrateur est l'installation du dispositif sur un port PCI de la carte mère. Les deux rôles distincts existants sont donc le rôle utilisateur côté zone basse et le rôle utilisateur côté machine haute.

[H.PRECAUTIONS_EMPLOI] Les utilisateurs respectent les précautions d'emploi définies dans la documentation utilisateur.

[H.NON_COLLUSION] L'utilisateur de la machine haute est considéré de confiance. De ce fait :

- si l'utilisateur situé côté zone basse est un attaquant, il ne peut pas disposer de complice ayant accès à la machine haute.

- Si l'utilisateur situé côté zone basse est un utilisateur de confiance (par exemple le même utilisateur que celui situé coté machine haute), il ne peut faire des attaques volontaires et conscientes sur la machine haute.

2.5. DESCRIPTION DES DEPENDANCES PAR RAPPORT A DES MATERIELS, DES LOGICIELS ET/OU DES MICROPROGRAMMES DU SYSTEME QUI NE SONT PAS FOURNIS AVEC LE PRODUIT

Il n'existe pas de dépendance particulière, les systèmes validés sont spécifiés dans la documentation utilisateur, Windows (*a minima* XP SP3, 7 ou version supérieure) et Linux noyau 2.6 à partir du 2.6.31, gérant l'USB Mass Storage.

2.6. DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNES (UTILISATEURS FINAUX, ADMINISTRATEURS, EXPERTS…) ET DE LEUR ROLE PARTICULIER DANS L'UTILISATION DU PRODUIT

Lors de la fabrication, les fonctions du produit sont figées et ne sont plus modifiables par la suite. Les deux rôles existants sont donc les rôles utilisateur côté zone basse et utilisateur côté machine haute.

2.7. DEFINITION DU PERIMETRE DE L'EVALUATION, A SAVOIR LES CARACTERISTIQUES DE SECURITE DU PRODUIT CONCERNEES PAR L'EVALUATION

Le périmètre de l'évaluation couvre la totalité du dispositif SCOOP, considéré en « boîte noire » sous l'angle de ses deux interfaces USB et PCI, une interface côté zone basse et une interface côté machine haute (cf. Figure 1).

L'objectif de sécurité principal du dispositif SCOOP-MS consiste à protéger l'accès à la machine haute depuis une connexion de périphérique USB accessible en zone basse, tout en permettant des échanges au travers de ces périphériques, limités à un transfert de données unidirectionnel depuis la zone basse vers la machine haute, avec un filtrage restrictif sur le format des données transférées.

3. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE D'EVALUATION

3.1. MATERIEL COMPATIBLE OU DEDIE

Présence d'un contrôleur et d'un emplacement PCI disponible sur la machine haute.

3.2. SYSTEME D'EXPLOITATION COMPATIBLE : TYPE, VERSION, CORRECTIFS…

Windows (XP SP3, 7 ou version supérieure) ou Linux noyau 2.6 à partir du 2.6.31, gérant l'USB Mass Storage.

L'environnement technique d'évaluation sera composé d'un Windows 7 et d'un Linux noyau 3.2.0 gérant l'USB Mass Storage.

4. DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

Le produit est conçu pour protéger les biens sensibles suivants :

- **[D.MHAUTE]** Données présentes sur la machine haute
- **[D.RESEAU_HAUT]** Toutes les données et machines accessibles par rebond du côté de la machine haute
- **[D.CONFIG_FILTRAGE]** Paramètres de configuration et de filtrage du dispositif
- **[D.TRANSFERT]** Données mises à disposition de la machine haute par le dispositif SCOOP

On considère (cf. §2.2.1) que les données en provenance du dispositif de stockage de masse de la zone basse ne sont pas des biens sensibles, e.g. non confidentiels.

5. DESCRIPTION DES MENACES

L'agent menaçant est tout utilisateur pouvant se connecter sur le port USB de la carte SCOOP-MS.

Les menaces contre lesquelles protège le dispositif SCOOP-MS sont les suivantes :

- **[M. INTRUSION_BAS>HAUT]** Tentative de prise de contrôle de la machine haute depuis la zone basse via le dispositif SCOOP.
- **[M. TRANSFERT_DONNEES_ILLICITES_BAS>HAUT]** Transfert de données non autorisées (cf. §6, F.FILTRAGE_FORMAT) depuis la zone basse vers la machine haute
- **[M. MODIF_CONFIG_SCOOP]** Modification de la configuration du dispositif via les seules interfaces accessibles du dispositif, à savoir le port USB.
- **[M. TRANSFERT_ILLICITE_HAUT>BAS]** Transfert illicite de données depuis la machine haute vers la zone basse

6. DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

Les fonctions de sécurité du produit sont les suivantes :

- **[F.TRANSFERT_UNIDIR]** Transfert unidirectionnel de données depuis le dispositif de stockage de masse utilisateur vers la machine haute et interdiction des transferts de données depuis la machine haute vers ce dispositif. Cette fonction peut être assimilée à une diode.
- **[F.FILTRAGE_FORMAT]** Filtrage du format des données transférées (transfert de fichiers au format texte, ne comportant que des caractères ayant un code ASCII défini dans des intervalles déterminés (décrits dans la documentation utilisateur), avec une longueur de

ligne limitée à un nombre maximum de caractères. Ces fichiers de type « texte » ont une taille limitée et une extension caractéristique.)

- **[F.PROTECTION_CONFIG_FILTRAGE]** Protection contre les tentatives de modification / altération de la configuration du dispositif via les seules interfaces accessibles du dispositif, à savoir le port USB.

7. VULNERABILITES IDENTIFIEES A CE JOUR

Aucune vulnérabilité connue.