Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2013/02

SCOOP-MS v1.0

Paris, le 26 février 2013

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

[ORIGINAL SIGNE]
Patrick Pailloux

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CSPN-2013/02

Nom du produit

SCOOP-MS

Référence/version du produit

V1.0

Catégorie de produit

Anti-virus
Protection contre les codes malveillants

Critères d'évaluation et version

CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)*

Développeur

SECLAB FR

300, rue Auguste Broussonet
34090 Montpellier
France

Commanditaire

EDF R&D

1, Av. du Général de Gaulle
F-92141 Clamart Cedex
France

Centre d'évaluation

Amossys

4 bis, allée du Bâtiment
35000 Rennes
France

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est **« SCOOP-MS v1.0 »** développé par SECLAB FR.

Le produit SCOOP-MS (Selective COntrol Of Peripherals - Mass Storage) est un dispositif de filtrage se présentant sous la forme d'une carte au format PCI. Il permet le transfert unidirectionnel de données entre un dispositif de stockage de masse (par exemple une clé USB), destiné à exporter des informations depuis la zone basse, et une machine située en zone haute. Il permet le passage d'informations du dispositif de stockage vers la machine haute via un point de stockage relais physique (inclus dans le produit), avec des restrictions sur les données échangées : filtrage selon le format des fichiers (contrôle de l'extension par liste blanche), selon les caractères contenus (contrôle du code ASCII) etc.
Le transfert des informations depuis le point de stockage relais vers la zone haute est toujours à l'initiative de cette dernière. On considère que le dispositif SCOOP-MS est le seul point d'entrée entre la zone basse et la zone haute.

1.2. Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1. Catégorie du produit

☐ 1 - détection d'intrusions
☒ **2 - anti-virus, protection contre les codes malicieux**
☐ 3 – firewall
☐ 4 - effacement de données
☐ 5 - administration et supervision de la sécurité
☐ 6 - identification, authentification et contrôle d'accès
☐ 7 - communication sécurisée
☐ 8 - messagerie sécurisée
☐ 9 – stockage sécurisé
☐ 10 - matériel et logiciel embarqué
☐ **99- Autres : environnement d'exécution sécurisé**

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans le fichier « debug.txt » présent sur le disque SC-DEBUG, monté par le dispositif à son initialisation. La capture d'écran suivante permet d'identifier le produit évalué :

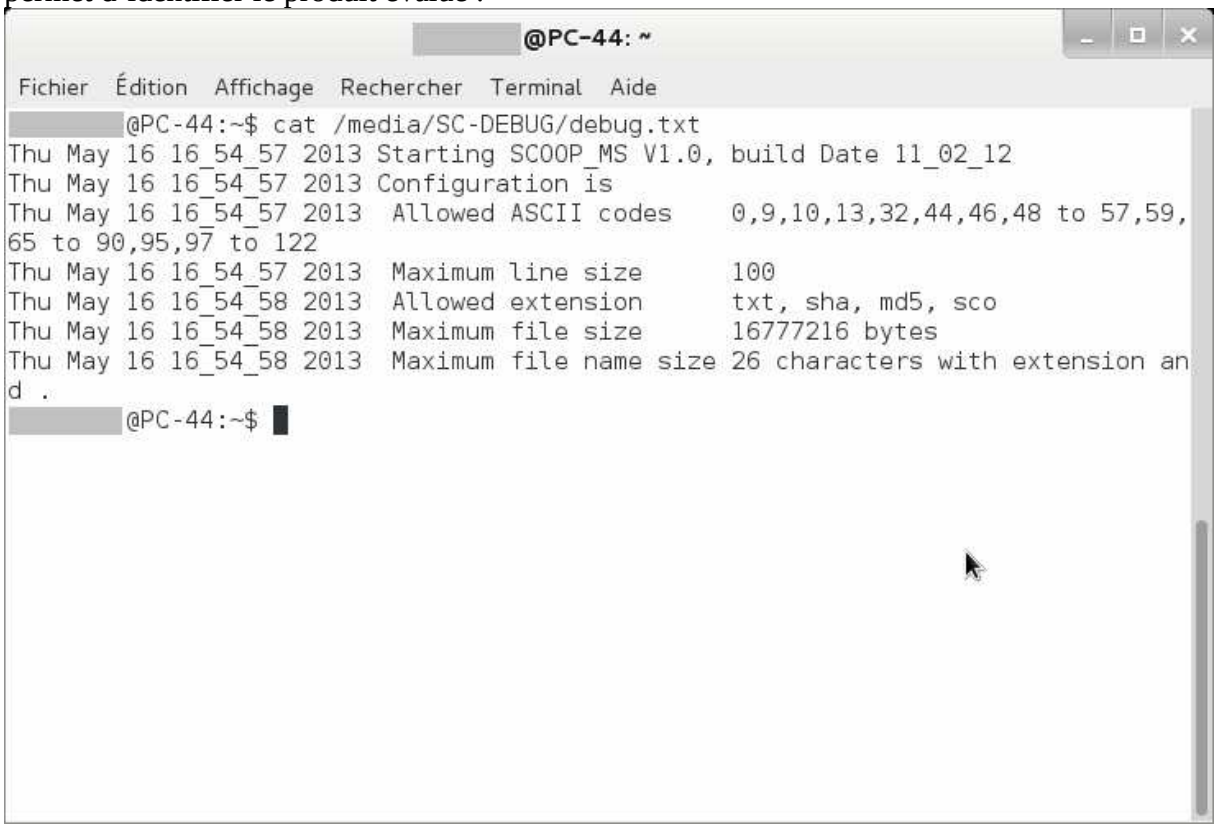

Figure 1 - Identification du produit

1.2.3. Services de sécurité

Le dispositif SCOOP-MS offre principalement les trois services de sécurité suivants :

- transfert unidirectionnel de données depuis le dispositif de stockage de masse de l'utilisateur vers la machine en zone haute et interdiction des transferts de données en sens inverse ;
- filtrage du format des données transférées : le dispositif n'autorise que les fichiers de type texte correspondant à une extension reconnue (filtrage par liste blanche) ; les extensions non autorisées sont modifiées afin, le cas échéant, que les fichiers ne puissent plus être exécutés sans la complicité de l'utilisateur de la zone haute. De plus, quel que soit le type de fichier, le contenu est filtré et seuls les caractères dont le code ASCII est autorisé sont copiés vers la zone haute, les autres étant remplacés par le caractère « _ ». Les détails concernant la configuration de la fonction de filtrage figurent dans [GUIDES] ;
- protection contre les tentatives de modification/altération de la configuration du dispositif via les seules interfaces accessibles du dispositif, à savoir le port USB.

1.2.4. Configuration évaluée

Comme indiqué au chapitre 2.3.2.6, la configuration du dispositif SCOOP-MS est figée lors de la phase de développement et ne peut être modifiée par la suite.
La configuration évaluée est celle correspondant aux options de contrôle et de filtrage définies ci-après :

- contrôle du « *USB device class* » ;
- contrôle du nom de fichier (longueur/caractères) ;
- liste blanche de formats de fichiers (contrôle de l'extension) ;
- contrôle de la taille globale des données transférées et/ou des fichiers ;
- contrôle du contenu : uniquement les caractères autorisés ;
- contrôle de la longueur des lignes.

2. L'évaluation

2.1. Référentiels d'évaluation

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

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit ne comportant pas de mécanismes cryptographiques, soit 25 hommes x jours.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 2 « Argumentaire (description) du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 4 « Description des biens sensibles que le produit doit protéger »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (chapitre 5 « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 6 « Description des fonctions de sécurité du produit »).

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 2.6 « Description des utilisateurs typiques concernés et de leur rôle particulier dans l'utilisation du produit »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

Comme illustré ci-dessous, la plate-forme de test est composée d'un PC situé en zone basse (**EVL**) et de trois PC situés en zone haute et équipés du dispositif SCOOP-MS (**SC1, SC2 et SC3)**.

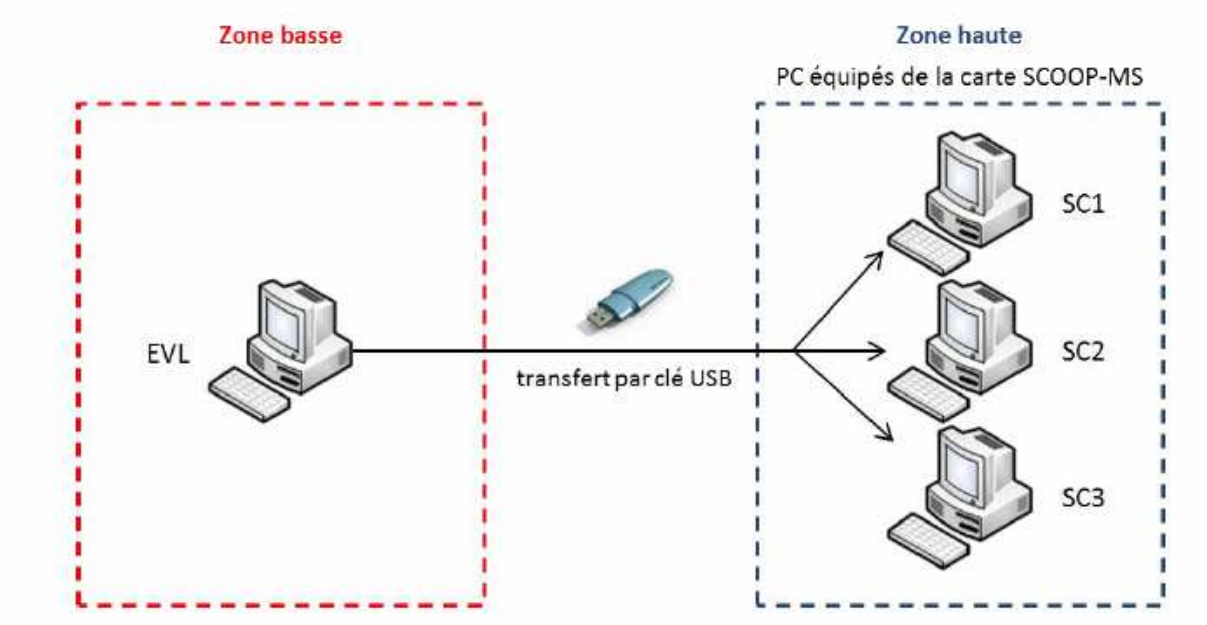

Figure 2 : Plateforme de test

Le PC EVL est utilisé pour générer du contenu, enregistré sur la clé USB présentée ensuite aux dispositifs SCOOP-MS équipant les PC SC1 à SC3. Le PC EVL est supposé situé en zone basse tandis que les PC SC1, SC2 et SC3 correspondent à des machines situées en zone haute.

La configuration des différentes machines de test est la suivante :

- SC1 : Linux Debian Wheezy (noyau 3.235-2 x86_64 (3.2.0-4-amd64)) 64 bits, équipée du dispositif SCOOP-MS ;
- SC2 : Windows 7 Enterprise edition SP1, équipée du dispositif SCOOP-MS ;
- SC3 : Linux Debian Squeeze (noyau 2.6.32) 64 bits, équipée du dispositif SCOOP-MS ;
- EVL : Linux Debian Wheezy 64 bits.

2.3.2.2. Particularités de paramétrage de l'environnement

La machine destinée à accueillir le dispositif SCOOP-MS doit disposer d'un port PCI. En outre, l'espace disponible dans le prolongement de ce port doit être suffisant au regard des dimensions imposantes de la carte.
Enfin la carte SCOOP-MS ne nécessite aucune installation de logiciel spécifique ni aucun paramétrage particulier.

2.3.2.3. Options d'installation retenues pour le produit

Sans objet.

2.3.2.4. Description de l'installation et des non-conformités éventuelles

L'évaluateur a eu accès à la documentation technique du produit. La documentation est claire et détaillée, aucune non-conformité n'a été relevée.

2.3.2.5. Durée de l'installation

L'installation du produit ne nécessite que quelques minutes pourvu que la machine dispose de suffisamment d'espace libre dans le prolongement du port PCI.

2.3.2.6. Notes et remarques diverses

Il est à noter que le dispositif SCOOP-MS est entièrement configuré et figé lors de sa fabrication (hypothèse H.INIT). Aucune configuration n'est nécessaire au moment de l'installation ou lors de son utilisation, de fait il ne requiert aucune action de la part de l'administrateur.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire, concise et complète et aucune non-conformité n'a été relevée.

2.3.4. Revue du code source (facultative)

L'évaluateur n'a pas eu accès au code source.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Transfert unidirectionnel de données depuis la zone basse vers la zone haute	**Réussite**
Filtrage des formats et du contenu des fichiers	**Réussite**
Protection de la configuration contre l'altération ou la modification	**Réussite**

2.3.6. Fonctionnalités non testées

Sans objet.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

L'évaluateur a constaté que le caractère « tabulation » était filtré par le dispositif, contrairement à ce qu'affirme la documentation fournie par le développeur. Cette non-conformité ne remet néanmoins pas en cause le verdict global sur la fonction de filtrage.

2.3.8. Avis d'expert sur le produit

Le fonctionnement du dispositif est conforme à ses spécifications fonctionnelles.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Transfert unidirectionnel de données depuis la zone basse vers la zone haute
Filtrage des formats et du contenu des fichiers

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Le produit SCOOP-MS est fonctionnel et résistant à la plupart des attaques mais son comportement semble parfois instable sous environnement Linux, où l'évaluateur a mis en évidence la possibilité d'un déni de service sur le dispositif. Cependant, l'évaluateur n'a pas pu dans ce cas mettre en défaut les fonctions de sécurité du dispositif.
De plus, si un attaquant met le système dans un état instable ou inutilisable, une simple pression sur le bouton de réinitialisation présent en façade permet de remettre le système dans un état fonctionnel.
Ces problèmes n'ont pas été constatés sur l'environnement Windows 7 utilisé lors de l'évaluation.
La désactivation du port série, utilisé en usine pour la configuration de la carte, rend toute modification des paramètres de filtrage impossible ainsi que l'a vérifié l'évaluateur.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilités connues sur ce produit particulier.

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

L'évaluateur a mis en évidence la possibilité d'obtenir un déni de service sur la machine haute en stressant la fonction de filtrage du dispositif. Ce comportement n'a toutefois pas pu être reproduit de façon systématique et semble limité à certaines plateformes Linux. En outre l'évaluation n'a pas permis de mettre en lumière un scénario d'exploitation compatible avec un niveau CSPN.
De plus, un déni de service peut être obtenu sur la carte lors du montage d'un dispositif USB dont le système de fichier est corrompu ou, si l'hypothèse de non-collusion n'est pas respectée, en manipulant les disques virtuels SC-DEBUG et SC-READY.

2.3.11. Accès aux développeurs

Au cours de l'évaluation, les évaluateurs ont eu accès au développeur du produit. Au cours des échanges techniques qui ont eu lieu, le développeur a fait preuve d'une très bonne maîtrise de son produit et a été en mesure de répondre rapidement aux questions posées.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Le produit s'avère simple à utiliser, il n'est pas paramétrable ou configurable et n'induit pas de cas où la sécurité est ambiguë.

2.3.12.2. Recommandations pour une utilisation sûre du produit

La machine « haute » sur laquelle le produit est installé doit héberger un système d'exploitation à jour concernant les correctifs de sécurité et correctement configuré (mise en place d'une politique de gestion de supports, authentification robuste), administré et supervisé.

Le respect de l'hypothèse de non-collusion est en outre essentiel dans la perspective d'une utilisation sûre du produit. En effet, plusieurs attaques sont jouables avec la complicité de l'utilisateur en zone haute, du fait notamment de l'impossibilité de filtrer systématiquement un code malveillant (le dispositif le rendra cependant non exécutable par modification des permissions et de l'extension), ou de l'éventuelle exploitation d'un déni de service sur le dispositif.

Dans tous les cas les recommandations présentes dans [GUIDES] doivent être appliquées.

2.3.12.3. Avis d'expert sur la facilité d'emploi

Pour l'utilisateur final, l'utilisation de SCOOP-MS est simple, et ne nécessite aucun paramétrage ni aucune configuration de la part d'un administrateur.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

Sans objet.

2.5. Analyse du générateur d'aléas

Sans objet.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « SCOOP-MS v1.0 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le présent rapport et dans l'ensemble des guides [GUIDES].

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN – SCOOP-MS* ; Référence CR-I2D-2012-047 ; Date : 30/10/2012.
[RTE]	*RTE CSPN Produit SCOOP-MS* ; Référence : *CSPN-RTE-SCOOP-MS-v1-1.02* ; Version : *1.02* ; Date : 07/01/2013.
[GUIDES]	SCOOP-MS : *Documentation utilisateur*, version 1.0 ; Date : 02/11/2012.

Annexe 2. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr