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-2016/07

Balabit
Shell Control Box
Version 4.0.6.sec3

Paris, le 12 mai 2016

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

Guillaume POUPARD
[ORIGINAL SIGNE]

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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2016/07**
Nom du produit **Shell Control Box**
Référence/version du produit **Version 4.0.6.sec3**
Référence de la cible de sécurité **Cible de securite** **Référence : SCB 4 LTS, version 4.2 en date du 2 février 2016.**
Catégorie de produit **Identification, authentification et contrôle d'accès**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Commanditaire **Balabit** **Alíz street 2. H-1117 Budapest, Hungary**
Centre d'évaluation **Oppida** **4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France**
Fonctions de sécurité évaluées **Contrôle des accès aux serveurs cibles** **Traçabilité des accès aux serveurs cibles** **Protection des pistes d'audit** **Authentification des clients** **Authentification des administrateurs** **Protocoles sécurisés**
Fonctions de sécurité non évaluées **Néant**
Restrictions d'usage **Oui (cf. §3.2)**

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 le « Shell Control Box (SCB), version 4.0.6.sec3 » développé par *BALABIT*. Le rôle du produit est de contrôler les accès que les clients font sur les serveurs, en filtrant les demandes d'accès au niveau applicatif (couche 7 du modèle OSI[1]). Pour cela il est paramétré pour faire office de passerelle afin d'authentifier les clients. Ces derniers étant à la fois des utilisateurs et des machines. Le contrôle d'accès a également pour effet une journalisation des activités permettant à l'administrateur de surveiller tous les accès.

Dans le cadre de l'évaluation seule une partie du produit a été évaluée et une configuration particulière a été prise en compte.

La figure ci-dessous explicite l'architecture du produit.

Figure 1 - Architecture Produit.

[1] *Open System Interconnection*, standard de communication réseau.

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 – environnement d'exécution sécurisé
☐ 11 – matériel et logiciel embarqué
☐ 12 – terminal de réception numérique (Set top box, STB)
☐ 13 – automate programmable industriel

1.2.2. Identification du produit

Nom du produit	Shell Control Box
Numéro de la version analysée	4.0.6.sec3

Le produit soumis à évaluation était une image ISO contenu sur un CDROM, prête à être installée sur une machine. Outre le produit, cette image ISO contient également un système d'exploitation (Ubuntu). Les empreintes de cette image ISO sont les suivantes :

SHA-1	a4d7fc7faff9b05cd50002c8ccacac6ddc70c944
SHA-256	f2bcd24a5bdbde2edce6a7c9dd13989eaddbbe6ed59b6da6b9c1347a984ee635

La version certifiée du produit peut être identifiée de trois façons différentes :

- avant installation : la version du produit est affichée en haut de l'écran d'installation. Il y a également dans cette interface d'installation un menu permettant l'affichage de la version (« *Version Information* ») ;
- après installation : au travers de la console administrateur local, le message d'accueil indique la version installée ;
- après installation : à travers l'accès administrateur distant (HTTPS), un onglet dédié dans menu « *Basic Settings / system* » indique la version installée.

1.2.3. Configuration évaluée

Le produit Shell Control Box est disponible sous deux formes : appliance matérielle ou appliance virtuelle. La configuration évaluée correspond à une appliance virtuelle, comme mentionné dans la [CDS].

Le produit est capable de filtrer plusieurs protocoles de communications (SSHv2, X11, VMware View, RDP, Telnet, VNC, Citrix ICA, etc.), mais pour l'évaluation seul le protocole SSH a été pris en compte. Ainsi, seul ce protocole fait l'objet de la certification.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. 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 dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, menaces, utilisateurs et fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Plateforme de test

Le produit a été installé dans une machine virtuelle.

2.3.1.2. Particularités de paramétrage de l'environnement et options d'installation

La configuration évaluée nécessite des paramétrages spécifiques qui ne sont pas activées par défaut, à savoir :

- configuration en mode bastion. Dans ce mode, les clients peuvent uniquement se connecter au produit SCB, l'accès direct au serveur est impossible, quel que soit le protocole de communication utilisé entre le client et le serveur ;

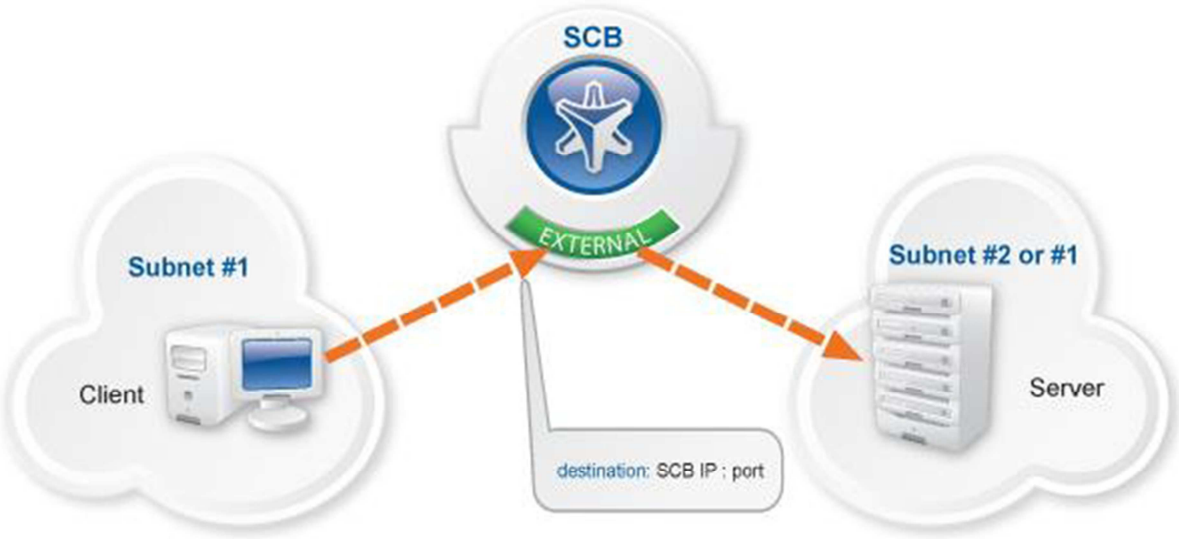

Figure 2: Configuration évaluée

- activation du chiffrement, de la signature et de l'horodatage des traces d'audit ;

- activation de l'option « *Seal the box* », permettant de restreindre l'accès à distance des administrateurs au protocole HTTPS seulement ;
- activation du proxy SSH avec authentification par mot de passe local pour les utilisateurs/clients.

Comme précisé dans la section 1.2.3 les autres services que le produit est capable de filtrer ne sont pas activés et donc pas évalués.

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

L'installation se fait à partir d'une image ISO. Cette dernière contient un installateur guidé (« *wizard* ») permettant l'installation du système d'exploitation et du produit.

2.3.1.4. Durée de l'installation

L'installation sous forme de machine virtuelle est courte, de l'ordre de la demi-heure.

2.3.1.5. Notes et remarques diverses

Il est à noter qu'il est nécessaire de générer des clés cryptographiques et des certificats pour l'authentification de l'interface d'administration et pour le chiffrement et la signature des traces d'audit.

2.3.2. Analyse de la documentation

La documentation couvre tous les points pouvant poser problème lors de la configuration du produit. En effet, l'évaluation a montré qu'il n'est pas toujours évident de correctement configurer le produit sans utilisation de la documentation. Pour cela, cette dernière apporte des exemples et semble clairement distinguer les cas où la sécurité du produit peut être remise en cause, au travers d'explications préfixées par des pictogrammes.

2.3.3. Revue du code source (facultative)

Le code source de la cible d'évaluation n'a pas été fourni.

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité ont été testées et sont conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation dans la cible de sécurité [CDS].

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Il n'a pas été identifié de vulnérabilité connue et exploitable sur ce produit.

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

L'évaluation a mis en avant les vulnérabilités suivantes :

- le port SNMP est ouvert par défaut et fourni des informations sur le système ;
- il est possible de faire des attaques par force-brute sur l'authentification utilisateur ;

- il est possible, dans une moindre mesure, de faire des attaques par force brute sur l'authentification administrateur.

Cependant, les recommandations décrites en section 2.3.8.2 permettent de rendre ces vulnérabilités non exploitables.

2.3.7. Accès aux développeurs

Néant.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

Le produit, ainsi que la documentation accompagnant ce dernier, définit comme mot de passe fort une chaîne de 8 caractères. Cette longueur n'est pas suffisante pour tous les mots de passe que le produit manipule, et plus particulièrement ceux de l'administrateur et du compte *root*.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Il est important de prendre en compte les recommandations suivantes pour une utilisation sûre du produit :

- tous les mots de passe (utilisateur/client, administrateur, compte *root*) doivent avoir une longueur et une complexité conforme au Référentiel général de sécurité [RGS] ;
- les journaux doivent être surveillés par l'administrateur afin de se prémunir contre les attaques de type force-brute ;
- l'agent SNMP doit être durci, voire totalement désactivé s'il n'est pas indispensable au client final ;
- les composants logiciels utilisés par le produit doivent être maintenus à jour.

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

L'installation du produit est simple, car guidée. Par contre la configuration du produit semble plus complexe. Il est important de se référer à la documentation accompagnant le produit afin de correctement configurer la TOE.

2.3.8.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

L'évaluateur a procédé à une analyse des mécanismes cryptographiques implémentés par le produit. Celle-ci n'a pas relevé de manquements jugés bloquants, néanmoins l'évaluateur a mis en évidence une non-conformité due à l'utilisation de la fonction de compression MD5 pour la dérivation de clé. Compte tenu de la complexité du chemin d'attaque cela ne remet pas en cause le niveau global de la sécurité du produit.

2.5. Analyse du générateur d'aléas

Néant.

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 « Shell Control Box, version 4.0.6.sec3 » 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. Cependant l'évaluation a mis en avant des restrictions d'usage à respecter strictement pour une utilisation sécurisée du produit décrites ci-après :

- le mode « *Seal the box* » doit être activé ;
- le chiffrement, de la signature et de l'horodatage des traces d'audit doit être activé ;
- le proxy SSH avec authentification par mot de passe local pour les utilisateurs/clients doit être activé ;
- les autres services de filtrage ne doivent pas être activés (et donc être bloqués par le produit) ;
- tous les mots de passe (utilisateur/client, administrateur, compte *root*) doivent avoir une longueur et une complexité conforme au Référentiel général de sécurité [RGS] ;
- les journaux doivent être surveillés par l'administrateur afin de se prémunir contre les attaques de type force-brute ;
- l'agent SNMP doit au minimum voir sa configuration durcie, voire être désactivé s'il n'est pas indispensable au client final ;
- les composants logiciels utilisés par le produit doivent être maintenus à jour.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Security_Target_Balabit_SCB_V4.0 - update2016-02-02* Version : *4.2* ; Date : *02 février 2016*
[RTE]	*Rapport Technique d'Évaluation (RTE) CSPN BALABIT3* Référence : *OPPIDA/CESTI/BALABIT3/RTE/1.1* ; Version : 1.1 ; Date : *29 avril 2016*

Annexe 2. Références 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 des produits (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur http://www.ssi.gouv.fr/
[REF-CRY]	Référentiel général de sécurité, version 2.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03. Documents disponibles sur http://www.ssi.gouv.fr/
[GUIDE-ANSSI]	Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013. Disponible sur www.ssi.gouv.fr/hygiene-informatique.
[RGS]	Référentiel général de sécurité, version 1.0, annexe B3 : Règles et recommandations concernant les mécanismes d'authentification, version 1.0. Documents disponibles sur http://www.ssi.gouv.fr/