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-2013/05

Dropbear
Version 2012.55

Paris, le 17 mai 2013

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

Patrick Pailloux
[ORIGINAL SIGNE]

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-2013/05**
Nom du produit **Dropbear**
Référence/version du produit **2012.55**
Catégorie de produit **Communication sécurisée**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **Matt Johnston** **https://matt.ucc.asn.au/dropbear/dropbear.html**
Commanditaire **Quarkslab** **71-73, avenue des Ternes** **75017 Paris** **France**
Centre d'évaluation **Quarkslab** **71-73, avenue des Ternes** **75017 Paris**

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 « Dropbear, version 2012.55 » développé par Matt Johnston.

Ce produit est composé d'un serveur et d'un client SSH. Le protocole SSH est un protocole de communication sécurisé entre deux systèmes permettant aux utilisateurs de se connecter à des serveurs distants et d'obtenir un terminal ou exécuter des commandes sur le système cible.

Plus particulièrement, Dropbear est conçu pour remplacer OpenSSH dans des environnements avec de faibles ressources mémoire et processeur, comme des systèmes embarqués par exemple.

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

1.2.2. Identification du produit

La version certifiée du produit est identifiable par les fichiers d'installation identifiés dans [GUIDES].

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'authentification du serveur ;
- l'authentification du client ;
- la confidentialité et l'intégrité des communications.

1.2.4. Configuration évaluée

La configuration évaluée est celle par défaut.

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 comportant des mécanismes cryptographiques, soit 35 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 »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

L'architecture nécessaire à la réalisation de l'évaluation a été déployée sur des machines virtuelles à l'aide du logiciel VMware ESXi, version 5.0.0. Les environnements sont en 64 bits uniquement (x86-64) et le système d'exploitation de toutes les machines virtuelles, ainsi que les services s'y exécutant possèdent l'ensemble des mises à jour disponibles au début de l'évaluation.

Le serveur Dropbear a été déployé sur une distribution Ubuntu 10.04 Server et le client Dropbear a été déployé sur une distribution Ubuntu 12.04 Desktop.

A des fins de tests d'interopérabilité, le serveur SSH OpenSSH est également installé sur le serveur afin de pouvoir y accéder à distance ; le port utilisé par OpenSSH est 22222[1] afin de ne pas interférer avec le port TCP 22 par défaut qui sera utilisé par Dropbear. Le client SSH OpenSSH est aussi installé sur le poste client.

2.3.2.2. Particularités de paramétrage de l'environnement

Sans objet.

2.3.2.3. Options d'installation retenues pour le produit

La procédure suivie pour installer le produit est celle par défaut, comme indiqué dans le fichier INSTALL.

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

Un environnement de développement est nécessaire pour compiler le produit, ainsi que la bibliothèque ZLIB.

Dropbear a été compilé depuis les sources téléchargées depuis le site de l'éditeur.

Aucune option particulière n'a été précisée lors de la compilation.

2.3.2.5. Durée de l'installation

L'installation dure moins de 10 minutes une fois les sources téléchargées.

2.3.2.6. Notes et remarques diverses

L'installation est simple et ne requiert aucune configuration de la part de l'utilisateur.

[1] Ce port a été choisi à des fins d'évaluation uniquement. Comme indiqué dans la règle 24 de [NOTE-SSH], il est recommandé de privilégier un port inférieur à 1024 pour un usage opérationnel.

2.3.3. Analyse de la documentation

Le produit ne dispose pas de guides à proprement parler mais la documentation est répartie entre plusieurs fichiers texte distincts à la racine du projet ainsi que dans les pages de manuel une fois le produit installé [GUIDES].

Cette documentation ne dispose pas de plan ou de mise en forme particulière. De part l'absence de centralisation des éléments de documentation et de la mauvaise organisation de leurs contenus, cette documentation vise un public d'administrateur étant habitué de l'environnement de compilation et d'installation Linux et ayant une bonne connaissance du système sur lequel le produit est destiné à être installé.

2.3.4. Revue du code source (facultative)

L'évaluateur a eu accès au code source, le code source est clair, documenté et homogène.

2.3.5. Fonctionnalités testées

Les fonctions suivantes ont été soumises à des tests de conformité :

Fonctionnalité	Résultat
Authentification par mot de passe	**Réussite**
Authentification avec un couple de clefs publique/privée	**Réussite**
Désactivation de l'authentification pour l'utilisateur root	**Réussite**
Chiffrement des données	**Réussite**
Utilisation des options *no-pty*, *no-agent-forward*, *no-port-forwarding*, *no-x11-forwarding*	**Échec**
Journalisation	**Réussite**

2.3.6. Fonctionnalités non testées

Sans objet.

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

L'ensemble des fonctionnalités testées s'est avéré globalement conforme à la cible de sécurité [CDS]. Mais un bogue provoque le crash du serveur lorsqu'une des options `no-pty`, `no-agent-forwarding`, `no-port-forwarding` ou `no-x11-forwarding` est présente dans le fichier `~/.ssh/authorized_keys` d'un utilisateur. Le bogue empêche un utilisateur de se connecter avec sa clé privée, mais la connexion est toujours possible par mot de passe.

2.3.8. Avis d'expert sur le produit

A l'exception du bogue évoqué ci-dessus, le produit est fonctionnellement conforme à sa cible de sécurité.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Les fonctions et mécanismes suivants ont été soumis à des tests de résistance et de pénétration :

Fonction et mécanisme
Négociation de la version du protocole et des logiciels utilisés
Négociation des algorithmes utilisés
Echange de la clé de session et contrôle de l'authenticité du serveur
Authentification de l'utilisateur
Echange de données sécurisé
Clôture de la connexion

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Il a d'abord été relevé un respect strict des différentes RFC associées au protocole SSH, son architecture et ses dépendances vis-à-vis de la cryptographie.

Par ailleurs, de nombreuses bonnes pratiques ont été mises en évidence en termes de gestion de la mémoire et des tampons (*buffers*) de données. Ainsi, le produit implémente à bas niveau la gestion sécurisée de tampons avec notamment la validation des dépassements des capacités. De plus, toute erreur critique d'allocation et de libération mémoire entraîne la fermeture immédiate du produit (client ou serveur).

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 applicables à cette version du produit.

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

Une vulnérabilité a été identifiée concernant la rémanence des secrets en mémoire. Cette vulnérabilité n'a pas été jugée exploitable dans le contexte d'utilisation de la cible de sécurité [CDS] pour un niveau d'attaquant attendu en CSPN.

Une vulnérabilité du produit a été identifiée sur les systèmes uClinux, il est donc déconseillé d'utiliser Dropbear sur ce système (cf. §2.3.12.1).

2.3.11. Accès aux développeurs

Les évaluateurs n'ont pas eu accès au développeur du produit durant l'évaluation.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

L'utilisation du produit sur un système uClinux ne permet pas d'atteindre un niveau de sécurité suffisant pour une CSPN.

De plus, il faut noter que les restrictions mises en place par utilisateur dans les fichiers `~/.ssh/authorized_keys` sont effectives uniquement lorsque l'utilisateur se connecte en utilisant sa clé publique. La connexion par mot de passe ne tient pas compte de ces restrictions.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Dropbear ne possédant pas de fonctionnalités pour chiffrer les clés privées, il est recommandé :

- de stocker les clés privées chiffrées, en utilisant un logiciel de chiffrement externe ;
- de privilégier l'authentification par mot de passe à l'authentification par clé publique lorsque les clés sont stockées en clair ;
- d'utiliser un autre client SSH, comme par exemple celui d'OpenSSH, lorsque les contraintes en ressources mémoires et processeurs ne concernent que la partie serveur.

Les clés générées devront respecter les référentiels de sécurité du RGS [REF-CRY] et être stockées sous forme chiffrée, protégée par un mot de passe.

Afin de permettre à l'utilisateur de pouvoir mettre en place des restrictions, le serveur doit être démarré avec l'option `-s` pour désactiver la connexion par mot de passe.

Enfin, le poste client doit héberger un système d'exploitation à jour concernant les correctifs de sécurité et être correctement administré. Le poste doit être durci afin d'être protégé contre des codes malveillants (voir le guide d'hygiène informatique [GUIDE-ANSSI], notamment ses règles 14 et 15).

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

Moyennant le respect des recommandations évoquées précédemment, l'évaluateur n'a pas identifié de cas où le produit serait configuré ou utilisé de façon non sûre mais qu'un utilisateur pourrait raisonnablement croire sûre.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

La liste de référence des mécanismes cryptographiques est celle fournie par la cible de sécurité [CDS]. La résistance de ces mécanismes a été analysée par l'évaluateur. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [RTE] et concluent que le produit met en œuvre des mécanismes cryptographiques conformes à [REF-CRY] auxquels il convient de se restreindre (cf. §2.3.12.2).

2.5. Analyse du générateur d'aléas

Le produit s'appuie sur le générateur d'aléas `/dev/urandom`. Dropbear étant amené à être installé sur un système embarqué, l'entropie accumulée à l'initialisation du système est potentiellement insuffisante pour être conforme au référentiel de l'ANSSI [REF-CRY]. Cependant, les moyens mis en œuvre pour le retraitement des nombres aléatoire permettent d'atteindre le niveau de résistance aux attaques visé par la CSPN.

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 « Dropbear**,** version 2012.55 **»** 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.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN – Dropbear 2012.55 ;* Référence : *12-06-037-CSPN-cible-dropbear* ; Date : *01/06/2012*
[RTE]	*Evaluation CSPN - Rapport technique d'évaluation ;* Référence : *12-06-038-CSPN-rte-dropbear* ; Date : *04/06/2012*
[GUIDES]	Guide d'installation L'installation est décrite dans plusieurs fichiers de documentation présents à la racine des sources : • le fichier *INSTALL*, décrivant l'installation ; • le fichier *MULTI*, décrivant la compilation ; • le fichier *README*, contenant diverses notes ; • le fichier *SMALL*, décrivant la création d'un binaire de taille minimal. Guide d'utilisation L'utilisation du produit est décrite dans les pages de manuel (*man*) des programmes *dbclient*, *dropbear* et *dropbearkey* une fois le produit installé.

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 (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.
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur 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. Document disponible sur www.ssi.gouv.fr/hygiene-informatique.
[NOTE-SSH]	Recommandations pour un usage sécurisé d'(Open)SSH, version 1.1 du 15 avril 2013. Document disponible sur www.ssi.gouv.fr.