Cible de sécurité CSPN

Dropbear 2012.55

Ref	**12-06-037-CSPN-cible-dropbear**
Version	**1.0**
Date	**June 01, 2012**

Quarkslab SARL
71 – 73 avenue des Ternes
75017 Paris
France

Table des matières

1. Identification

1.1 Identification de la cible de sécurité

La cible de sécurité CSPN du logiciel Dropbear 2012.55 a été rédigée par Quarkslab sur fonds propres.

Cette cible de sécurité a été élaborée en vue d'une évaluation Certification Sécurité de Premier Niveau (CSPN).

1.2 Identification du produit

Catégorie	**Identification**
Organisation éditrice	Matt Johnston
Lien vers l'organisation	https ://matt.ucc.asn.au/dropbear/
Nom commercial du produit	Dropbear
Numéro de la version évaluée	2012.55
Catégories de produit	identification, authentification et contrôle d'accès

2. Argumentaire (description) du produit

2.1 Description générale du produit

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 shell ou exécuter des commandes sur le système cible. Le protocole est ouvert et documenté par plusieurs RFC.

Dropbear est composé d'un serveur et d'un client **SSH2** conçus pour remplacer **OpenSSH** dans des environnements avec de faibles ressources mémoire et processeur, comme des systèmes embarqués par exemple.

Les fonctions de sécurité principales sont :
- La confidentialité et l'intégrité des communications : aucun paquet n'est transmis en clair sur le réseau grâce au chiffrement de la communication établi avant l'authentification du client.
- L'authentification du serveur : chaque connexion à un serveur SSH distant provoque la vérification de son identité.
- L'authentification du client par le serveur au moyen d'un mot de passe ou d'une clé privée.

2.2 Description de l'utilisation du produit

2.2.1 Serveur SSH

En tant que serveur SSH, Dropbear est généralement installé comme un service : il démarre avec le système et reste actif en permanence. Le port TCP par défaut du protocole SSH est le port 22.

2.2.2 Client SSH

Le client SSH Dropbear est utilisé pour se connecter à un serveur SSH distant. L'utilisateur a une interaction explicite avec Dropbear :
- lors de la création d'un couple de clés ;
- lors de la connexion à un système distant pour éventuellement vérifier la signature de la clé publique du serveur et entrer le mot de passe de l'utilisateur spécifié.

2.3 Description de l'environnement d'utilisation prévu

Dropbear fonctionne sur les systèmes **POSIX** suivants :
- **Linux**,

- **Mac OS X**,
- **FreeBSD**, **NetBSD** et **OpenBSD**,
- **Solaris**,
- **IRIX 6.5**,
- **Tru64 5.1**,
- **AIX 4.3.3**,
- **HPUX 11.00**,
- **Cygwin**.

2.4 Description des hypothèses sur l'environnement

2.4.1 Environnement logique

Le client et le serveur Dropbear doivent être installés sur des systèmes sains, correctement mis à jour, en particulier au niveau des correctifs liés à la sécurité. Il convient également de sécuriser les système, par désactivation des services et partages inutiles par exemple.

L'administrateur dispose des moyens de contrôler la configuration du client et du serveur Dropbear par rapport à un état de référence, ou de la régénérer dans un état sûr.

2.4.2 Environnement physique

Les équipements contenant le serveur Dropbear doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

2.4.3 Mesures organisationnelles

Les administrateurs sont des personnes considérées comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration.

2.5 Description des dépendances

La plupart sinon toutes les distributions majeures du système open source GNU/Linux intègrent d'origine Dropbear dans le système de paquets. Un environnement de développement et la bibliothèque **zlib** sont nécessaires pour compiler Dropbear depuis les sources.

2.6 Description des utilisateurs typiques

Le contexte d'utilisation du serveur Dropbear fait intervenir l'administrateur dans les étapes d'installation et de configuration du serveur. L'utilisateur peut influencer le com-

portement du serveur en plaçant des fichiers de configuration et des clés dans son répertoire personnel.

L'utilisateur typique du client Dropbear est l'utilisateur du compte géré par le système d'exploitation.

2.7 Définition du périmètre de l'évaluation

Dropbear est divisé en plusieurs programmes : le client, le serveur, et les programmes de gestion de clés.

Les principaux objectifs de l'évaluation sont de valider que l'identification effectuée par le serveur est effectuée de façon correcte, et que les fonctionnalités du client Dropbear ne peuvent pas être détournées lors de la connexion à un serveur malveillant.

3. Description de l'environnement technique de fonctionnement

3.1 Matériel compatible ou dédié

Aucune contrainte matérielle particulière.

Les matériels retenus pour l'évaluation du client et du serveur sont ceux compatibles avec les systèmes d'exploitation retenus ci-dessous. Il s'agit d'architectures standards de type x86-64 (64 bits) et x86 (32 bits).

3.2 Environnement système retenu

L'environnement de test sera composé de systèmes **`Linux`** :
– **`Ubuntu 10.04 Server`** pour le serveur,
– **`Ubuntu 12.04 Desktop`** pour le client.

3.3 La solution Dropbear

La solution Dropbear auditée est la version 2012.55 publiée le 22 février 2012.

4. Description des biens sensibles que le produit doit protéger

Le serveur Dropbear fournit un interpréteur de commandes sur le système distant ainsi qu'un transfert de connexion TCP en utilisant un moyen de communication sécurisé. Le produit contribue donc à protéger l'accès à un système distant et les communications entre le client et le serveur.

Les bien sensibles de Dropbear (clés privées, journaux d'évènements, etc.) doivent être protégés par le système d'exploitation sous lequel s'exécute Dropbear.

5. Description des menaces

Les menaces affectant le produit peuvent être classées en trois catégories distinctes :
– les menaces affectant le serveur depuis le réseau ou localement ;
– les menaces affectant le client ;
– les menaces affectant la solution de manière globale.

Par hypothèse, les administrateurs ne sont pas considérés comme des attaquants potentiels pour le serveur.

5.1 Menaces affectant le client

– Transmission d'un flux non autorisé sur le SI du client ;
– Connexion à un serveur *malicieux* : l'authenticité n'est pas respectée ;
– Établissement d'une connexion non sécurisée à l'insu du client : la confidentialité n'est pas respectée ;
– Faiblesse dans le stockage des clefs privées SSH.

5.2 Menaces affectant le serveur

– Déni de service ;
– Contournement de l'authentification ;
– Élévation de privilèges depuis un compte local.

5.3 Menaces affectant la solution de manière globale

– Attaque de type *Man-In-The-Middle* ;
– Déchiffrement des flux entre le client et le serveur.

Il est intéressant de valider l'implémentation et le comportement à l'exécution de ces différents types de fonctionnalité afin de détecter les éventuels manquements aux bonnes pratiques de sécurité.

6. Description des fonctions de sécurité du produit

Dropbear est constitué d'un client et d'un serveur **SSH** qui est principalement dédié à la fourniture d'un service d'accès distant en ligne de commande. Les fonctions de sécurité proposées par l'équipe en charge du projet sont les suivantes :

6.1 Authentification

- mécanisme d'authentification classique par mot de passe (via **PAM**) ;
- mécanisme d'authentification forte avec un couple de clef publique/privée de type **RSA** ou **DSA** ;
- désactivation de l'authentification pour l'utilisateur **root**.

6.2 Chiffrement

- utilisation du protocole SSH v2 (client et serveur).

6.3 Fonctions générales

- déconnexion des clients en cas d'inactivité prolongée ;
- redéfinition de la bannière par défaut ;
- désactivation des redirections de port (*port forwarding*) ;
- désactivation des redirections X11 (*X11 forwarding*).

6.4 Traçabilité

- utilisation de **syslog**.

Le produit n'a pas pour vocation à détecter les attaques qui pourraient être menées à son encontre, il doit cependant s'assurer par des mécanismes intrinsèques que les différents échanges et actions effectués sont réalisés de manière légitime.