



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 06 mai 2011
N° CERTA-2011-AVI-276

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenSSH

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-276>

Gestion du document

| | |
|-----------------------------|------------------------------|
| Référence | CERTA-2011-AVI-276 |
| Titre | Vulnérabilité dans OpenSSH |
| Date de la première version | 06 mai 2011 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité OpenSSH |
| Pièce(s) jointe(s) | Aucune |

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Atteinte à la confidentialité des données.

2 Systèmes affectés

OpenSSH, versions antérieures à 5.8p2.

3 Résumé

Une vulnérabilité pouvant conduire à la divulgation de clés privées a été découverte dans *OpenSSH*.

4 Description

Une vulnérabilité a été découverte dans *OpenSSH*. Elle peut conduire à la divulgation des clés privées de l'hôte.

Cette vulnérabilité est localisée dans *ssh-rand-helper*. Cet outil, seulement utilisé lorsque le système hôte ne dispose pas de source d'entropie interne, hérite d'un descripteur de fichier ouvert en lecture sur le fichier contenant les clés privées. Cet outil s'exécutant dans le contexte d'un utilisateur non privilégié, il est possible de s'y attacher pour ensuite lire les clés privées contenues dans le fichier pointé par le descripteur.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité *OpenSSH* :
<http://www.openssh.com/txt/portable-keysign-rand-helper.adv>

Gestion détaillée du document

06 mai 2011 version initiale.