

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-2006-AVI-100>

Gestion du document

Référence	CERTA-2006-AVI-100
Titre	Vulnérabilité dans OpenSSH
Date de la première version	03 mars 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité FreeBSD du 01 mars 2006
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

Déni de service à distance.

2 Systèmes affectés

- FreeBSD 5.3 ;
- FreeBSD 5.4.

3 Résumé

Une vulnérabilité dans OpenSSH permet à un utilisateur mal intentionné de provoquer un déni de service à distance.

4 Description

Une vulnérabilité dans la mise en oeuvre du protocole SSH peut être exploitée par un individu malveillant afin de provoquer un déni de service au moyen de connexions malicieusement réalisées.

5 Solution

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

6 Documentation

- Bulletin de sécurité FreeBSD SA-06-09 du 01 mars 2006 :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06-09.openssh.asc>
- Référence CVE CAN-2006-0883 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0883>

Gestion détaillée du document

03 mars 2006 version initiale.