

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de OpenSSH pour Debian

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-2008-AVI-466>

Gestion du document

Référence	CERTA-2008-AVI-466-001
Titre	Vulnérabilité de OpenSSH pour Debian
Date de la première version	18 septembre 2008
Date de la dernière version	16 octobre 2008
Source(s)	Bulletin de sécurité Debian DSA-1638 du 16 septembre 2008
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

OpenSSH server version 4.3p2-9etch2 inclus dans Debian 4.0.

3 Résumé

Une vulnérabilité présente dans le serveur OpenSSH de la version stable (*etch* ou 4.0) de la distribution GNU/Linux Debian permet à un utilisateur distant de provoquer un déni de service.

4 Description

Une vulnérabilité est présente dans le serveur OpenSSH utilisé dans la distribution GNU/Linux Debian 4.0. Elle est relative à la façon dont sont gérés les délais maximaux d'attente autorisés lors de la phase de connexion d'un client. Cette faille permet à un utilisateur distant de provoquer un déni de service du serveur vulnérable.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA-1638 du 16 septembre 2008 :
<http://www.debian.org/security/2008/dsa-1638>
- Bulletin de sécurité Ubuntu USN-649-1 du 01 octobre 2008 :
<http://www.ubuntu.com/usn/usn-649-1>
- Bulletin de sécurité SUSE SUSE-SR:2008:020 du 07 octobre 2008 :
<http://lists.opensuse.org/opensuse-security-announce/2008-10/msg0004.html>
- Référence CVE CVE-2008-4109 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4109>

Gestion détaillée du document

18 septembre 2008 version initiale ;

16 octobre 2008 ajout des bulletins de sécurité Ubuntu et SuSE.