Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 mars 2002
N° CERTA-2002-AVI-053

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de mémoire dans OpenSSH v2

Gestion du document

Référence	CERTA-2002-AVI-053
Titre	Débordement de mémoire dans OpenSSH v2
Date de la première version	12 mars 2002
Date de la dernière version	–
Source(s)	Liste de diffusion Bugtraq
Pièce(s) jointe(s)	Aucune

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

1 Risque

Elévation de privilèges d'un utilisateur légitime.

2 Systèmes affectés

OpenBSD, FreeBSD, toute distribution Linux et tout système utilisant OpenSSH dans une version comprise entre 2.0 et 3.0.2.

3 Résumé

Un utilisateur mal intentionné peut exécuter du code arbitraire avec les privilèges du service *sshd*, soit généralement *root*.

4 Description

Une mauvaise vérification de la taille d'un tampon permet un débordement de mémoire, exploitable après authentification, que ce soit sur le serveur *sshd* au profit d'un utilisateur mal intentionné, ou sur le client au travers d'un serveur malicieux.

5 Solution

- Télécharger et compiler la dernière version d'OpenSSH (au moins 3.1) depuis le site officiel : http://www.openssh.com
- Télécharger et installer le port/paquetage correspondant à la distribution lorsqu'il sera disponible :
  - Linux Red Hat 7.0 à 7.2 : http://www.redhat.com/support/errata/RHSA-2002-043.html
  - Linux Mandrake 7.1 à 8.1 : http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-019.php
  - Distribution Debian : SSHv1 uniquement, donc non concernée.
  - SuSE Linux 6.4 à 7.3 : http://www.suse.com/de/support/security/2002_009_openssh_txt.txt
  - Conectiva Linux 5.0 à 7.0 : http://distro.conectiva.com/atualizacoes/?id=a&anuncio=000467
  - FreeBSD : ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02%3A13.openssh.asc
  - OpenBSD : http://www.openbsd/advisories/ssh_channelalloc.txt

6 Documentation

- Avis original : http://www.pine.nl/advisories/pine-cert-20020301.txt

Gestion détaillée du document

12 mars 2002 version initiale.