



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 février 2001
N° CERTA-2001-AVI-017

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de SSH

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-2001-AVI-017>

Gestion du document

Référence	CERTA-2001-AVI-017
Titre	Vulnérabilité de SSH
Date de la première version	12 février 2001
Date de la dernière version	–
Source(s)	Bugtraq
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

Accès Root à distance.

2 Systèmes affectés

Tout système Unix possédant les versions SSH-1.2.24 à SSH-1.2.32 activées, ou OpenSSH antérieures à 2.3.0 et pour lesquelles la compatibilité SSH Version 1 est en fonction.

3 Résumé

Une vulnérabilité de SSH permet à un utilisateur mal intentionné d'accéder à un *shell* root à distance.

4 Description

Un utilisateur mal intentionné n'ayant pas de compte sur la machine cible peut, grâce à un débordement de mémoire de SSH, obtenir à distance l'accès à un *shell* ayant les privilèges root.

5 Solution

- Mettre à niveau SSH
<ftp://ftp.ssh.com/pub/ssh/>
- Pour Debian il est possible de télécharger la mise à jour de SSH :
<http://security.Debian.org/dists/stable/updates/main/>

6 Documentation

Avis de Sécurité Debian :
<http://www.debian.org/security/2001/dsa-027>

Gestion détaillée du document

12 février 2001 version initiale.