Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 octobre 2001
N° CERTA-2001-AVI-104-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités multiples dans l'implémentation OpenSSH du protocole SSH v2

Gestion du document

Référence	CERTA-2001-AVI-104-001
Titre	Vulnérabilités multiples dans l'implémentation OpenSSH du protocole SSH v2
Date de la première version	28 septembre 2001
Date de la dernière version	19 octobre 2001
Source(s)	Listes de diffusion BugTraq et openssh-unix-dev
Pièce(s) jointe(s)	Aucune

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

1 Risque

Contournement de la politique de sécurité.

2 Systèmes affectés

OpenBSD, FreeBSD, toute distribution Linux et tout système utilisant OpenSSHv2 dans une version inférieure à la 2.9.9.

3 Résumé

Un utilisateur mal intentionné peut contourner une configuration restreignant les adresses IP de connexion au serveur ou les commandes autorisées sur ce dernier.

4 Description

Le fichier *~/.ssh/authorized_keys2*, de chaque utilisateur autorisé à se connecter via SSH, permet de restreindre les actions permises et/ou l'adresse du client par l'ajout d'options à chaque clé publique listée.

Ces limitations sont souvent utilisées lorsque le client distant est invoqué automatiquement (tâche programmée,...) et que par conséquent sa clé privée n'est pas protégée par un mot de passe.

Dans certains cas particuliers, ces restrictions peuvent être contournées :

- si le serveur *sftp* (*ftp* sécurisé introduit avec la version 2) est lancé, il peut être invoqué malgré la restriction sur les commandes autorisées, et, selon les droits du client, être utilisé pour modifier le fichier *~/.ssh/authorized_keys2* dans le but d'obtenir un shell, par exemple.
- si 2 clés de nature différente (i.e. RSA et DSA) se suivent au sein de ce fichier, alors les options sur la seconde clé s'appliquent également à la première, ce qui peut conduire au non respect de restrictions sur l'adresse source du client pour la première clé.

5 Contournement provisoire

- Désactiver le lancement du sous-système *sftp* sur le serveur (usuellement dans le fichier *sshd_config*) dans le premier cas.
- Commenter l'une des clés ou créer de nouvelles clés de manière à unifier le type, dans le second cas.

6 Solution

- Télécharger et compiler la dernière version d'OpenSSH depuis le site officiel :
  http://www.openssh.org
- Télécharger et installer le port/paquetage correspondant à la distribution lorsqu'il sera disponible.
  - Linux Mandrake :
    http://www.linux-mandrake/en/security/2001/MDKSA-2001-081.php3
  - Linux Red Hat :
    http://www.redhat.com/support/errata/RHSA-2001-114.html
  - Linux Trustix :
    http://www.trustix.net/errata/misc/2001/TSL-2001-0026-openssh.as.txt

7 Documentation

- OpenSSH Security Advisory
  http://www.securityfocus.com/cgi-bin/archive.pl?id=1&mid=216702
- OpenSSH: sftp & bypassing keypair auth restrictions
  http://www.securityfocus.com/cgi-bin/archive.pl?id=1&mid=214921

Gestion détaillée du document

28 septembre 2001 version initiale.
19 octobre 2001 ajout de liens sur les distributions Linux de Mandrake, Red Hat et Trustix.