Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 décembre 2001
N° CERTA-2001-AVI-159

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Risque de compromission locale avec 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-2001-AVI-159

Gestion du document

Référence	CERTA-2001-AVI-159
Titre	Risque de compromission locale avec OpenSSH
Date de la première version	07 décembre 2001
Date de la dernière version	–
Source(s)	Rapport de vulnérabilité VU#157447 du CERT/CC 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 inférieure à la 3.0.2.

3 Résumé

Si la directive *UseLogin* a la valeur « yes », un utilisateur mal intentionné peut exécuter du code arbitraire avec les privilèges du démon *sshd*, soit généralement *root*.

4 Description

Le démon *sshd* peut invoquer *login* pour toute connexion interactive, si la directive *UseLogin* est positionnée à « yes » dans son fichier de configuration (usuellement */etc/sshd_config*). Par défaut, cette option n'est pas activée mais elle est cependant couramment utilisée.

Un utilisateur mal intentionné peut alors spécifier les variables d'environnement utilisées par *login* et ainsi exécuter du code arbitraire après une authentification par clé publique.

5 Contournement provisoire

Mettre la directive *UseLogin* à « no » si l'usage du système ne le requiert pas. Sinon, désactiver temporairement l'authentification par clé publique jusqu'à la mise à jour du système.

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 Red Hat :
    http://www.redhat.com/support/errata/RHSA-2001-161.html
  - Linux Debian :
    http://www.debian.org/security/2001/dsa-091
  - SuSE Linux :
    http://www.suse.com/de/support/security/2001_044_openssh_txt.txt
  - FreeBSD :
    ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01%3A63.openssh.asc
  - OpenBSD :
    http://archives.neohapsis.com/archives/openbsd/2001-12/0261.html
  - IBM AIX (utilisateurs enregistrés) :
    http://www6.software.ibm.com/aixtbx/aixtbx-p

7 Documentation

- Rapport de vulnérabilité VU#157447 du CERT/CC
  http://www.kb.cert.org/vuls/id/157447
- Avis BugTraq
  http://www.securityfocus.com/bid/3614
- Documentation du démon *sshd*
  http://www.openbsd.org/cgi-bin/man.cgi?query=sshd

Gestion détaillée du document

07 décembre 2001 version initiale.