Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 octobre 2006
N° CERTA-2006-AVI-453

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2006-AVI-453`

Gestion du document

Référence	CERTA-2006-AVI-453
Titre	Vulnérabilité de OpenSSH
Date de la première version	13 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité OpenBSD du 12 octobre 2006
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

Toutes les versions de OpenSSH antérieures à la 4.4.

3 Résumé

Une vulnérabilité présente dans OpenSSH permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Une erreur dans la mise en œuvre du serveur `sshd` de OpenSSH permet à un utilisateur distant de provoquer un déni de service sur le serveur vulnérable. En outre, si le support de l'autentification via `GSSAPI` (`Kerberos`) est activé dans `sshd`, il lui est alors possible d'exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 1189 du 04 octobre 2006 :
  http://www.debian.org/security/dsa-1189
- Bulletin de sécurité Mandriva MDKSA-2006:179 du 03 octobre 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:179
- Bulletin de sécurité RedHat RHSA-2006:0698 du 28 septembre 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0698.html
- Bulletin de sécurité RedHat RHSA-2006:0697 du 28 septembre 2006 :
  http://rhn.redhat.com/errata/RHSA-2006-0697.html
- Bulletin de sécurité Ubuntu USN-355-1 du 03 octobre 2006 :
  http://www.ubuntulinux.org/usn/usn-355-1
- Bulletin de sécurité FreeBSD SA-06:22.openssh du 30 septembre 2006 :
  ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:22.openssh.asc
- Référence CVE CAN-2006-5051 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-5051

Gestion détaillée du document

13 octobre 2006 version initiale.