

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans 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-411>

---

### Gestion du document

Référence	CERTA-2006-AVI-411-001
Titre	Vulnérabilité dans OpenSSH
Date de la première version	28 septembre 2006
Date de la dernière version	–
source(s)	Bulletin de sécurité Gentoo GLSA-200609-17 du 27 septembre 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

Déni de service à distance.

## 2 Systèmes affectés

- OpenSSH 3.x ;
- OpenSSH 4.x.

## 3 Résumé

Une vulnérabilité dans OpenSSH permet à un utilisateur distant mal intentionné de provoquer un déni de service à distance.

## 4 Description

Cette vulnérabilité n'est exploitable que si le support de la version 1 du protocole ssh est activé.

Une vulnérabilité causée par une erreur dans le traitement des paquets ssh ayant plusieurs block identiques permet de provoquer un déni de service en utilisant toutes les ressources du processeur. Cette vulnérabilité peut être exploitée au moyen d'un paquet ssh spécialement construit.

## 5 Contournement provisoire

Vérifier que la directive `Protocol` dans le fichier `sshd_config` est fixée à 2 et non à 1.

## 6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 7 Documentation

- Bulletin de sécurité Gentoo GLSA-200609-17 du 27 septembre 2006 :  
<http://www.gentoo.org/security/en/glsa/glsa-200609-17.xml>
- Mise à jour de sécurité OpenSSH du 16 septembre 2006 :  
<http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/deattack.c.diff?r1=1.29&r2=1.30&sortby=date&f=h>  
  
<http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/packet.c.diff?r1=1.143&r2=1.144&sortby=date&f=h>  
  
<http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/deattack.h.diff?r1=1.9&r2=1.10&sortby=date&f=h>
- Bulletin de sécurité SCO SCOSA-2008.2 du 12 mars 2008 :  
<ftp://ftp.sco.com/pub/unixware7/714/security/p534336/p534336.txt>
- Référence CVE CVE-2006-4924 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4924>

## Gestion détaillée du document

**28 septembre 2006** version initiale.

**28 septembre 2006** ajout de la section Contournement provisoire.

**13 mars 2008** ajout de la référence au bulletin de sécurité SCO.