

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans OpenSSH v2 et v3

---

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-2002-AVI-136>

---

### Gestion du document

Référence	CERTA-2002-AVI-136-001
Titre	Vulnérabilités dans OpenSSH v2 et v3
Date de la première version	27 juin 2002
Date de la dernière version	8 juillet 2002
Source(s)	Avis OpenSSH Avis CA-2002-18 du CERT/CC
Pièce(s) jointe(s)	Aucune

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

## 1 Risque

- Déni de service ;
- Exécution distante de code arbitraire avec les privilèges du service *sshd* (généralement *root*).

## 2 Systèmes affectés

Tout système utilisant OpenSSH dans des versions comprises entre 2.3.1p1 et 3.3.

## 3 Résumé

Deux vulnérabilités ont été découvertes dans la gestion des défis/réponses (protocole SSH2) interne à OpenSSH. L'une au moins permet à un utilisateur mal intentionné d'exécuter du code sur l'hôte du service *sshd*.

## 4 Description

Les vulnérabilités sont deux débordements de mémoire dans la gestion du nombre de réponses reçues durant une authentification par défi/réponse de type SKEY ou BSD\_AUTH (système d'authentification BSD) d'une part, et PAM (« Pluggable Authentication Modules » système modulaire de gestion de l'authentification présent entre autres sur la plupart des Linux et sur Sun Solaris) d'autre part.

## 5 Contournement provisoire

Appliquer au fichier de configuration de *sshd* (*sshd\_config*) au moins l'une des recommandations suivantes :

- Désactiver le support de SSH2 : *Protocol 1* ;
- Si la version d'OpenSSH est au moins 3.3, la directive *UsePrivilegeSeparation yes* limite les risques de compromission *root* (peut cependant affecter la compression sur les noyaux linux 2.2, rajouter alors *UseCompression no*) ;
- Désactiver le support des options de défi/réponse :
  - *ChallengeResponseAuthentication no*
  - *PAMAuthenticationViaKbdInt no* (versions supérieures à 2.9)
  - *KbdInteractiveAuthentication no* (versions comprises entre 2.3.1p1 et 2.9)

## 6 Solution

Mettre à jour OpenSSH avec une version au moins égale à la 3.4.

- Sources OpenSSH  
<http://www.openssh.com/>
- Mandrake Linux  
<http://www.linux-mandrake.com/en/secuirty/2002/MDKSA-2002-040.php>
- Debian  
<http://www.debian.org/security/2002/dsa-134>
- SuSE Linux  
<http://archives.neohapsis.com/archives/linux/suse/2002-q2/11166.html>
- Conectiva Linux  
<http://distro.conectiva.com/atualizacoes/?id=a&anuncio=00500>
- OpenWall Linux (version « current »)  
<http://www.openwall.com/Owl/>
- OpenBSD  
<http://www.openbsd.org/errata.html#sshd>
- FreeBSD  
<ftp://ftp.FreeBSD.org/pub/FreeBSD/branches/-current/ports/security/openssh/>
- Sun Solaris 9  
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?type=0&doc=fsalert%2F45525&display=plain>
- Sun Cobalt RaQ 550  
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?type=0&doc=fsalert%2F45508&display=plain>

## 7 Documentation

- Avis OpenSSH  
<http://www.openssh.com/txt/preauth.adv>
- Avis CA-2002-18 du CERT/CC  
<http://www.kb.cert.org/vuls/id/369347>
- Avis ISS  
<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20584>

## Gestion détaillée du document

**27 juin 2002** version initiale.

**8 juillet 2002** ajout des bulletins Sun.