



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 23 décembre 2002  
N° CERTA-2002-AVI-278

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans diverses implémentations SSH

---

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-278>

---

### Gestion du document

Référence	CERTA-2002-AVI-278
Titre	Vulnérabilités dans diverses implémentations SSH
Date de la première version	23 décembre 2002
Date de la dernière version	–
Source(s)	Avis CA-2002-36 du 16 décembre 2002 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 de code arbitraire à distance.

## 2 Systèmes affectés

Parmi les divers vendeurs affectés, les suivants ont officiellement reconnu un problème conséquent :

- certains routeurs Cisco et commutateurs Catalyst ;
- clients PuTTY pour Windows jusqu'à la version v0.53 ;
- clients SecureNetTerm pour Windows jusqu'à la version 5.4.1 ;
- serveur SecureShell de Pragma Systems jusqu'à la version 2 ;
- client Windows WinSCP 2.0.

## 3 Résumé

La société *Rapid7* a développé une suite de tests de charge pour le protocole SSHv2. Divers produits évalués se sont alors révélés vulnérables.

## 4 Description

Les tests portent sur l'initialisation de la connexion : échange de versions puis de clefs. La plupart des failles relèvent d'une mauvaise gestion des tampons mémoires. Ce type de problème conduit généralement à l'arrêt du processus quand il ne permet pas d'injecter du code qui sera exécuter avec les permissions du programme.

## 5 Contournement provisoire

- Pour les serveurs : restreindre les adresses IPs autorisées à se connecter à des adresses de «confiance» au moyen de listes de contrôle d'accès (ACL - «Access Control Lists») sur les routeurs ou en filtrant au niveau d'un pare-feu.
- Pour les clients : ne se connecter qu'à des serveurs de «confiance».

## 6 Solution

- Cisco : voir le bulletin de sécurité au paragraphe suivant ;
- PuTTY : mettre à jour avec une version au moins égale à 0.53b,  
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- SecureNetTerm : mettre à jour avec une version au moins égale à 5.4.2,  
<http://www.secureneterm.com>
- SecureShell : mettre à jour avec une version au moins égale à 3,  
<http://www.pragmasys.com>

## 7 Documentation

- Avis CA-2002-36 du 16 décembre 2002 du CERT/CC :  
<http://www.cert.org/advisories/CA-2002-36.html>
- Avis de sécurité Cisco du 19 décembre 2002 :  
<http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml>
- Communiqué F-Secure du 18 décembre 2002 :  
[http://www.f-secure.com/support/technical/ssh/ssh2\\_ca-2002-36.shtml](http://www.f-secure.com/support/technical/ssh/ssh2_ca-2002-36.shtml)
- Communiqué SSH Communications Security du 18 décembre 2002 :  
<http://www.ssh.com/company/newsroom/article/303/>

## Gestion détaillée du document

23 décembre 2002 version initiale.