

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans PuTTY

---

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-2004-AVI-267>

---

### Gestion du document

Référence	CERTA-2004-AVI-267-001
Titre	Vulnérabilité dans PuTTY
Date de la première version	05 août 2004
Date de la dernière version	06 août 2004
Source(s)	Bulletin de sécurité CORELABS CORE-2004-0705
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.

## 2 Systèmes affectés

PuTTY versions 0.54 et antérieures.

## 3 Résumé

Une vulnérabilité présente dans le logiciel PuTTY permet à un individu mal intentionné d'exécuter du code arbitraire à distance avec les droits de l'utilisateur ayant démarré PuTTY.

## 4 Description

PuTTY est une mise en œuvre libre de Telnet et SSH pour les plates-formes Windows et Linux.

Une vulnérabilité présente dans PuTTY permet à un individu mal intentionné d'exécuter du code arbitraire à partir d'un serveur SSH sur la machine se connectant à l'aide de PuTTY par l'envoi de paquets TCP malicieusement formés durant la phase d'authentification au serveur.

## 5 Solution

Mettre à jour PuTTY avec la version 0.55 qui corrige ces vulnérabilités :  
<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

## 6 Documentation

- Annonce de sécurité PuTTY du 03 août 2004 :  
<http://www.chiark.greenend.org.uk/~sgtatham/putty/changes.html>
- Bulletin de sécurité CORELABS CORE-2004-0705 du 04 août 2004 :  
<http://www.coresecurity.com/common/showdoc.php?idx=417&idxseccion=10>
- Bulletin de sécurité Gentoo GLSA 200408-04 du 5 août 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200408-04.xml>

## Gestion détaillée du document

**05 août 2004** version initiale.

**06 août 2004** ajout de précisions et de l'avis Gentoo.