

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de l'application Stunnel

---

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-2003-AVI-130>

---

### Gestion du document

Référence	CERTA-2003-AVI-130
Titre	Vulnérabilité de l'application Stunnel
Date de la première version	31 juillet 2003
Date de la dernière version	–
Source(s)	Avis de sécurité RedHat RHSA-2003:221-01
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.

## 2 Systèmes affectés

Stunnel versions 3.24 et antérieures et versions 4.03 et antérieures.

## 3 Résumé

Une vulnérabilité de l'application Stunnel permet à un utilisateur mal intentionné de provoquer un déni de service.

## 4 Description

Stunnel est une application utilisée pour encapsuler des connexions réseau. Elle permet de créer un tunnel sécurisé en utilisant SSL/TLS.

Lorsque l'application Stunnel est en écoute des connexions entrantes (sans être invoquée par *xinetd*), elle peut être configurée pour lancer soit un fil d'exécution (*thread*), soit un processus fils. Dans le second cas, un signal SIGCHLD sera reçu lorsque le processus fils sera lancé.

Une mauvaise gestion des signaux SIGCHLD par l'application permet à un utilisateur mal intentionné de provoquer un déni de service.

## **5 Solution**

Appliquer le correctif de votre éditeur.

## **6 Documentation**

Avis de sécurité RedHat RHSA-2003:221-01 :  
<http://www.redhat.com/apps/support/errata/>

Référence CVE CAN-2002-1563 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1563>

## **Gestion détaillée du document**

**31 juillet 2003** version initiale.