



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 janvier 2002
N° CERTA-2002-AVI-010

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2002-AVI-010>

Gestion du document

| | |
|-----------------------------|-----------------------------------|
| Référence | CERTA-2002-AVI-010 |
| Titre | Vulnérabilité dans stunnel |
| Date de la première version | 22 janvier 2002 |
| Date de la dernière version | – |
| Source(s) | Buletin de sécurité RHSA-2002:002 |
| 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 d'un code arbitraire à distance.

2 Systèmes affectés

stunnel de la version 3.15 à la version 3.21.c.

3 Résumé

stunnel est un utilitaire qui permet de détourner les canaux de communication classiques en les redirigeant dans un tunnel sécurisé.

Une vulnérabilité présente dans stunnel permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Un administrateur malveillant peut, en utilisant une vulnérabilité de type "chaîne de format", forcer l'exécution d'un code arbitraire à distance avec les privilèges de l'utilisateur du processus `stunnel`.

Cette vulnérabilité n'est exploitable qu'en mode client : utilisation de `stunnel` avec l'option `-n service` et l'option `-c` (mode client).

5 Solution

Installer la version 3.22 disponible sur le site

<http://www.stunnel.org> .

Des correctifs sont également disponibles sous forme de paquetages pour les distributions Linux (cf. section Documentation).

6 Documentation

- Avis de sécurité RHSA-2002:002 de RedHat :
<http://www.redhat.com/support/errata/RHSA-2002-002.html>
- Avis de sécurité MDKSA-2002:004 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-004.php>

Gestion détaillée du document

22 janvier 2002 version initiale.