

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-2003-AVI-203>

Gestion du document

Référence	CERTA-2003-AVI-203
Titre	Vulnérabilité dans Stunnel
Date de la première version	1er décembre 2003
Date de la dernière version	–
Source(s)	–
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

Usurpation du service légitime par un utilisateur local.

2 Systèmes affectés

Stunnel versions :

- antérieures à et incluant la 3.24,
- 4.00.

3 Résumé

Un serveur habilement construit, lancé par l'intermédiaire de *Stunnel*, peut arriver à remplacer ce dernier en écoute. Il est alors possible pour le propriétaire du serveur d'attenter à la confidentialité des échanges normalement sécurisés par *Stunnel* (mots de passe,...).

4 Description

Stunnel est un programme permettant de sécuriser une connexion réseau TCP en créant un tunnel SSL/TLS.

Une mauvaise gestion des descripteurs de fichiers sensibles permet à un utilisateur local mal intentionné de remplacer le service *Stunnel* par le sien. Un exploit est disponible.

5 Solution

Mettre à jour *Stunnel*.

- Sources 3.26 ou 4.04 au moins :
<http://stunnel.mirt.net/downloads.html>
- RedHat Linux
<http://rhn.redhat.com/errata/RHSA-2003-297.html>
- Mandrake Linux
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:108>

6 Documentation

Référence CVE CAN-2003-0740

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0740>

Gestion détaillée du document

1er décembre 2003 version initiale.