Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 février 2002
N° CERTA-2002-AVI-022

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du serveur ProFTPD

Gestion du document

Référence	CERTA-2002-AVI-022
Titre	Vulnérabilités du serveur ProFTPD
Date de la première version	04 février 2002
Date de la dernière version	–
Source(s)	Avis de securité Linux Mandrake MDKSA-2002-005
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

- Contournement des règles de sécurité ;
- Déni de service.

2 Systèmes affectés

Serveur FTP ProFTPD.

3 Résumé

Deux vulnérabilités présentes dans le serveur ProFTPD permettent à un utilisateur mal intentionné soit de contourner les Listes de Contrôle d'Accès (ACL), soit de provoquer un déni de service sur le serveur.

4 Description

- Première vulnérabilité :

Une erreur dans la vérification de la concordance entre l'adresse IP et le nom de la machine du serveur ProFTPD au niveau DNS permet à un utilisateur distant mal intentionné de contourner la liste de contrôle d'accès.

– Seconde vulnérabilité :
Un utilisteur distant, par le biais de certaines commandes envoyées au serveur ProFTPD, peut augmenter la consommation des ressources CPU et mémoire entraînant ainsi l'arrêt du serveur.

5 Contournement provisoire

– Première vulnérabilité :
Désactiver l'option `UserReverseDNS` du serveur.
– Seconde vulnérabilité :
Utiliser l'option `DenyFilter _*.*/` du serveur.

6 Solution

– Mettre à jour ProFTPD avec la version 1.2.2rc1 :
ftp://ftp.proftpd.org/distrib.source
– Correctif pour Linux Mandrake :
http://www.linux-mandrake.com/en/security

7 Documentation

Avis de securité Mandrake :
http://www.linux-mandrake.com/en/security/2002/MDKSA-2002-005.php

Gestion détaillée du document

04 février 2002 version initiale.