

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de ProFTPD

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-2006-AVI-524>

Gestion du document

Référence	CERTA-2006-AVI-524
Titre	Multiples vulnérabilités de ProFTPD
Date de la première version	04 décembre 2006
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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- *ProFTPD 1.3.0a* et versions antérieures.

3 Résumé

ProFTPD est un serveur de transfert de fichier pour le protocole FTP (RFC 959). Plusieurs vulnérabilités permettent de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Un débordement de mémoire permet à un utilisateur distant de provoquer un déni de service à distance. Une preuve d'exploitation existe sur l'Internet.

Un débordement de mémoire dans une fonction du module `mod_tls` permet d'exécuter un code arbitraire à distance. L'attaquant doit spécifier une longueur de données de valeur élevée.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Mandriva MDKSA-2006:271-1 du 30 novembre 2006 :
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:271-1>
- Référence CVE CVE-2006-5815 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5815>
- Référence CVE CVE-2006-6170 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6170>
- Référence CVE CVE-2006-6171 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6171>

Gestion détaillée du document

04 décembre 2006 version initiale.