

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans 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-2010-AVI-531>

---

### Gestion du document

Référence	CERTA-2010-AVI-531
Titre	Vulnérabilités dans ProFTPD
Date de la première version	03 novembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité ProFTPD du 29 octobre 2010
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 ;
- atteinte à l'intégrité des données.

## 2 Systèmes affectés

ProFTPD versions 1.3.0 à 1.3.3b.

## 3 Résumé

Deux vulnérabilités affectent *ProFTPD*. L'exploitation réussie de celles-ci permet, entre autre, l'exécution de code arbitraire à distance.

## 4 Description

Deux vulnérabilités ont été corrigées dans *ProFTPD*.

La première provient d'un débordement de pile lorsque l'utilisateur envoie au serveur une chaîne d'échappement spécifique. Lorsqu'elle est réussie, cette attaque permet l'exécution de code arbitraire à distance.

La seconde vulnérabilité se situe dans le module `mod_site_misc`. Si une personne malintentionnée a des droits d'accès en écriture à un répertoire, elle peut ensuite modifier des fichiers et des répertoires auxquels elle n'aurait théoriquement pas accès.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité ProFTPD du 29 octobre 2010 :  
<http://www.proftpd.org/docs/NEWS-1.3.3c>
- Référence CVE CVE-2010-3867 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3867>

## **Gestion détaillée du document**

**03 novembre 2010** version initiale.