Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 décembre 2006
N° CERTA-2006-AVI-561-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de ProFTPd

Gestion du document

Référence	CERTA-2006-AVI-561-001
Titre	Vulnérabilité de ProFTPd
Date de la première version	18 décembre 2006
Date de la dernière version	20 décembre 2006
Source(s)	Bulletin Securityfocus 21587
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 ;
- élévation de privilège.

2 Systèmes affectés

ProFTPD versions 1.2.x et 1.3.x compilées avec le module `mod_ctrls`.

3 Résumé

Une vulnérabilité permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance.

4 Description

ProFTPD est un serveur FTP libre. Le module `mod_ctrls` gère les communications par *sockets* entre le démon `proftpd` et le serveur Unix. Une mauvaise gestion de limite dans la fonction `pr_ctrls_recv_request()` peut être utilisée pour créer un débordement de mémoire. Cette vulnérabilité permet à un utilisateur malintentionné d'élever ses privilèges et d'exécuter du code arbitraire en envoyant un message de commande spécialement conçu au module vulnérable.

5 Contournement provisoire

Désactiver le module par l'insertion des lignes suivantes dans le fichier de configuration `proftpd.conf` :

```
<ifModule mod_ctrls.c>
ControlsEngine off
</ifModule>
```

Utiliser les listes de contrôle d'accès (*ACL*) pour n'accorder le droit d'envoyer des messages de commande au module `mod_ctrls` qu'aux utilisateurs de confiance.

6 Solution

La version 1.3.1rc1 corrige la vulnérabilité. Se référer au site de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Site du projet ProFTPD :
  http://www.proftpd.org/index.html
- Bulletin de sécurité Mandriva MDKSA-2006:232 du 18 décembre 2006 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2006:232
- Référence CVE CVE-2006-6563 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6563
- Bulletin Securityfocus 21587 du 15 décembre 2006 :
  http://securityfocus.com/bid/21587/info

Gestion détaillée du document

18 décembre 2006 version initiale.
20 décembre 2006 ajout de la référence au bulletin de sécurité Mandriva.