Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 mai 2004
N° CERTA-2003-AVI-155-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de ProFTPD

Gestion du document

Référence	CERTA-2003-AVI-155-002
Titre	Vulnérabilité de ProFTPD
Date de la première version	26 septembre 2003
Date de la dernière version	12 mai 2004
Source(s)	Avis de sécurité ISS X-Force du 23/09/2003
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.

2 Systèmes affectés

- ProFTPD versions 1.2.7 et antérieures ;
- ProFTPD 1.2.8 ;
- ProFTPD 1.2.8rc1 ;
- ProFTPD 1.2.8rc2 ;
- ProFTPD 1.2.9rc1 ;
- ProFTPD 1.2.9rc2.

3 Résumé

Une vulnérabilité dans `ProFTPD` permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

ProFTPD est un serveur FTP (File Transfer Protocol). Un débordement de mémoire est déclenché lors du téléchargement en mode ASCII d'un fichier habilement constitué et préalablement déposé sur le serveur ProFTPD. Il est alors possible pour un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

5 Contournement provisoire

Interdire le dépôt de fichiers sur le serveur ProFTPD. Editer le fichier de configuration de ProFTPD comme suit :

```
<Limit WRITE>
   DenyAll
</Limit>
```

6 Solution

Les versions disponibles sur le site de ProFTPD corrigent cette vulnérabilité :
ftp://ftp.proftpd.org

7 Documentation

- Site Internet de ProFTPD :
  http://www.proftpd.org
- Avis de sécurité de ISS X-Force du 23 septembre 2003 :
  http://xforce.iss.net/xforce/alerts/id/154
- Avis de sécurité Mandrake MDKSA-2003:095 :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:095
- Avis de sécurité FreeBSD du 05 janvier 2004 :
  http://www.vuxml.org/freebsd/
- Mise à jour de sécurité du paquetage NetBSD proftpd :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities
- Référence CVE CAN-2003-0831 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0831

Gestion détaillée du document

26 septembre 2003 version initiale.
30 septembre 2003 ajout de la référence CVE et du bulletin de sécurité Mandrake.
12 mai 2004 ajout des références aux bulletins de sécurité FreeBSD et NetBSD.