

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans *ftpd* et *ProFTPD* sur FreeBSD

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-2011-ALE-007>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2011-ALE-007-001 |
| Titre | Vulnérabilité dans <i>ftpd</i> et <i>ProFTPD</i> sur FreeBSD |
| Date de la première version | 02 décembre 2011 |
| Date de la dernière version | 26 décembre 2011 |
| 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 ;
- élévation de privilèges.

2 Systèmes affectés

- *ftpd* fourni avec FreeBSD versions 8.2 et inférieures ;
- *ftpd* fourni avec FreeBSD versions 8.2 amd64 et inférieures ;
- *ProFTPD* sur FreeBSD.

3 Résumé

Une vulnérabilité présente dans *ftpd* et *ProFTPD* sur FreeBSD permet à une personne malintentionnée distante d'exécuter du code arbitraire avec les privilèges administrateur (*root*).

4 Description

Une vulnérabilité est présente dans *ftpd* et *ProFTPD* sur FreeBSD. Elle permet à un utilisateur malintentionné distant d'exécuter du code arbitraire avec les privilèges administrateur (*root*). L'attaque est possible si :

- l'attaquant est en mesure de se connecter au serveur FTP en utilisant un compte utilisateur valide qui sera dans un environnement cloisonné (*chroot*), ou en tant qu'utilisateur anonyme avec les droits en écriture dans son répertoire racine ;
- le compte FTP utilisé possède les droits en écriture dans les répertoires `lib` et `etc` ou peut les créer s'ils n'existent pas.

L'attaque consiste à copier des fichiers, dont une bibliothèque malveillante dans le répertoire `lib`. La bibliothèque malveillante est ensuite chargée lorsqu'une commande FTP particulière est effectuée.

Une preuve de faisabilité est disponible sur Internet.

5 Contournement provisoire

Supprimer les droits en écriture sur les dossiers `lib` et `etc` permet d'empêcher l'attaquant de déposer les fichiers nécessaires à l'exploitation de la vulnérabilité.

6 Solution

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

7 Documentation

- Avis de sécurité FreeBSD FreeBSD-SA-11:07 du 23 décembre 2011 :
<http://security.freebsd.org/advisories/FreeBSD-SA-11:07.chroot.asc>

Gestion détaillée du document

02 décembre 2011 version initiale.

26 décembre 2011 ajout des correctifs FreeBSD.