

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de 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-2004-AVI-374>

---

### Gestion du document

Référence	CERTA-2004-AVI-374
Titre	Vulnérabilité de FreeBSD
Date de la première version	22 novembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité FreeBSD FreeBSD-SA-04:16.fetch du 18 novembre 2004
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

Toutes les versions de FreeBSD.

## 3 Résumé

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

## 4 Description

`fetch` est un utilitaire permettant le téléchargement de fichiers en utilisant les protocoles FTP, HTTP et HTTPS.

Une vulnérabilité de type débordement d'entier dans l'analyse des en-têtes HTTP permet à un utilisateur mal intentionné, en créant une réponse aux en-têtes habilement constitués, d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

## **5 Contournement provisoire**

En attendant l'application du correctif, ne pas utiliser l'utilitaire `fetch` mais l'utilitaire `ftp` (présent dans la base du système FreeBSD) qui n'est pas affecté par cette vulnérabilité.

## **6 Solution**

Se référer au bulletin de sécurité de FreeBSD pour l'obtention du correctif (cf. section Documentation).

## **7 Documentation**

Bulletin de sécurité FreeBSD FreeBSD-SA-04:16.fetch du 18 novembre 2004 :  
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:16.fetch.asc>

## **Gestion détaillée du document**

**22 novembre 2004** version initiale.