



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 21 octobre 2004  
N° CERTA-2004-AVI-272-004

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités du serveur tnftpd

---

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-272>

---

### Gestion du document

Référence	CERTA-2004-AVI-272-004
Titre	Vulnérabilités du serveur tnftpd
Date de la première version	19 août 2004
Date de la dernière version	21 octobre 2004
Source(s)	Bulletin de sécurité NetBSD-SA2004-009 du 17 août 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 avec les droits de l'administrateur *root*.

## 2 Systèmes affectés

- Versions du serveur tnftpd antérieures à la version 20040810 ;
- versions du serveur NetBSD-ftp antérieures à la version 20040809 ;
- toutes les versions du serveur lukemftpd.

## 3 Résumé

De multiples vulnérabilités du serveur FTP *lukemftpd / tnftpd /ftpd (Heimdal)* permettent à un utilisateur d'obtenir les droits de l'administrateur *root*.

## 4 Description

Le serveur *lukemftpd / tnftpd /ftpd (Heimdal)* est un serveur FTP pour les plates-formes FreeBSD, NetBSD et MacOSX. On le retrouve également dans certaines distributions Linux.

Ce serveur n'est pas installé par défaut sur les plates-formes FreeBSD et NetBSD.

Plusieurs vulnérabilités ont été découvertes sur le serveur FTP *lukemftpd* / *tnftpd* / *ftpd* (*Heimdal*). Elles permettent à un utilisateur distant d'exécuter du code arbitraire avec les privilèges de l'utilisateur *root*.

Si le serveur est lancé avec l'option "-r", l'attaquant n'obtiendra que les droits d'un utilisateur *ftp* non privilégié.

## 5 Solution

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

## 6 Documentation

- Site Internet du projet *tnftpd* :  
<http://freshmeat.net/projects/tnftpd/>
- Bulletin de sécurité FreeBSD pour *tnftpd* du 17 août 2004 :  
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité NetBSD pour *tnftpd* NetBSD-SA2004-009 du 17 août 2004 :  
<ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-009.txt.asc>
- Bulletin de sécurité Apple du 07 septembre 2004 :  
<http://docs.info.apple.com/article.html?artnum=61798>
- Mise à jour de sécurité du paquetage NetBSD *tnftpd* :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/tnftpd/README.html>
- Bulletin de sécurité Heimdal du 13 septembre 2004 :  
<http://www.pdc.kth.se/heimdal/advisory/2004-09-13/>
- Mise à jour de sécurité du paquetage NetBSD *heimdal* :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/security/heimdal/README.html>
- Bulletin de sécurité Debian DSA-551 du 21 septembre 2004 :  
<http://www.debian.org/security/2004/dsa-551>
- Bulletin de sécurité Sun #57655 du 15 octobre 2004 :  
<http://www.sunsolve.sun.com/search/document.do?assetkey=1-26-57655-1>
- Référence CVE CAN-2004-0794 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0794>

## Gestion détaillée du document

**19 août 2004** version initiale.

**08 septembre 2004** ajout de la référence au bulletin de sécurité Apple et de la référence CVE.

**15 septembre 2004** ajout de la référence au bulletin de sécurité Heimdal et à la mise à jour de sécurité du paquetage NetBSD heimdal.

**22 septembre 2004** ajout de la référence au bulletin de sécurité Debian.

**21 octobre 2004** ajout de la référence au bulletin de sécurité Sun #57655 pour *ftpd* (*Heimdal*) livré avec Sun Java Desktop System (JDS).