Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 novembre 2007
N° CERTA-2007-AVI-476

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans gFTP

Gestion du document

Référence	CERTA-2007-AVI-476
Titre	Multiples vulnérabilités dans gFTP
Date de la première version	05 novembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Secunia du 2 novembre 2007
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 ;
- déni de service à distance.

2 Systèmes affectés

Les versions de gFTP utilisant la bibliothèque fpslib antérieure à la version 0.9.

3 Résumé

gFTP est un client FTP utilisant une bibliothèque contenant deux vulnérabilités.

4 Description

Le logiciel gFTP est un client graphique *ftp* pour l'interface GNOME. Pour offrir la compatibilité avec le protocole *FPS* (*File service Protocol*), il utilise la bibliothèque fpslib qui contient deux vulnérabilités concernant le traitement des noms longs de répertoire. Une personne malveillante peut exécuter du code arbitraire sur la machine d'un utilisateur, lorsque ce dernier accède à un serveur contenant des noms de répertoire spécifiquement formés, à l'aide du client gFTP.

5 Solution

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

6 Documentation

- Bulletin de sécurité Gentoo GLSA-200711-01 du 01 novembre 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200711-01.xml
- Alerte de Secunia numéro 26378 du 09 août 2007 :
  http://secunia.com/advisories/26378/
- Alerte de Secunia numéro 27501 du 02 novembre 2007 :
  http://secunia.com/advisories/27501/
- Référence CVE CVE-2007-3961 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3961
- Référence CVE CVE-2007-3962 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3962

Gestion détaillée du document

05 novembre 2007 version initiale.