Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 avril 2001
N° CERTA-2001-AVI-043

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la fonction glob() dans les serveurs FTP

Gestion du document

Référence	CERTA-2001-AVI-043
Titre	Vulnérabilité de la fonction glob() dans les serveurs FTP
Date de la première version	11 avril 2001
Date de la dernière version	–
Source(s)	Avis CA-2001-07 du CERT CC
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.

2 Systèmes affectés

Serveurs FTP suivants :

- FreeBSD 4.2 ;
- Fujitsu UXP/V ;
- HP-UX 11 ;
- NetBSD 1.5 ;
- OpenBSD 2.8 ;
- SGI IRIX 6.5.x ;
- Solaris 8.

3 Résumé

Un utilisateur distant mal intentionné peut, par l'emploi des caractères de substitution, exécuter du code arbitraire sur le serveur cible.

4 Description

Une fonction glob permet, lors de la consultation d'un serveur ftp, de mettre des caractères de substitution, tels que « * » ou « ~ », dans les noms des fichiers.

L'utilisation de ces caractères permet, par exemple lors de l'utilisation de la commande « mget *.c », de récupérer tous les fichiers portant l'extension « .c ».

Une vulnérabilité dans la fonction glob(), lors de l'utilisation conjointe des caractères « * » et « ~ », peut provoquer un débordement de pile. Un utilisateur mal intentionné effectuant une requête, avec des caractères de substitution judicieusement placés, peut provoquer l'exécution de code arbitraire avec les droits du serveur ftp (trop souvent root).

5 Solution

- Procédure de mise à jour et correctif NetBSD :
  ftp://ftp.netbsd.org/pub/NetBSD/misc/security/advisories/NetBSD-SA2001-005.txt.asc
- FreeBSD n'a pas diffusé de correctif mais FreeBSD 5.0-CURRENT et FreeBSD 4.2-STABLE du 10 avril 2001 n'est pas vulnérable.
  ftp://ftp.freebsd.org/pub/FreeBSD
- Pour les autres plates formes, les correctifs ne sont actuellement pas disponibles.

Recommandation : Lancer le serveur ftp en tant qu'utilisateur afin de diminuer les droits.

6 Documentation

Avis du CERT CC :
http://www.cert.org/advisories/CA-2001-07.html

Gestion détaillée du document

11 avril 2001 version initiale.