Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 novembre 2001
N° CERTA-2001-AVI-153-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de wu-ftpd

Gestion du document

Référence	CERTA-2001-AVI-153-001
Titre	Vulnérabilité de wu-ftpd
Date de la première version	29 novembre 2001
Date de la dernière version	03 décembre 2001
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 ;
- élévation de privilèges.

2 Systèmes affectés

Toutes les versions du serveur wu-ftpd jusqu'à la version 2.6.1 incluse, y compris certaines versions *Beta* 2.7.0. wu-ftpd est livré avec la plupart des distributions Linux.

3 Résumé

Une vulnérabilité du serveur wu-ftpd permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine.

4 Description

Une vulnérabilité de la fonction *glob* utilisée par le serveur wu-ftpd permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine.

Si le compte *anonymous* du serveur FTP est désactivé, l'utilisateur doit pouvoir s'authentifier auprès du serveur pour exploiter cette vulnérabilité.

5 Contournement provisoire

En attendant d'appliquer les correctifs, arrêter le serveur wu-ftpd, ou filtrer le port 21/tcp au niveau des gardes-barrières pour limiter l'exploitation de cette vulnérabilité.

6 Solution

Pour la version 2.6.1, il faut appliquer tous les correctifs présents dans le répertoire suivant :
ftp://ftp.wu-ftpd.org/pub/wu-ftpd-attic/wu-ftpd-2.6.1-patches/

La version 2.6.2 n'est pas vulnérable et est disponible sur le site de wu-ftpd.

Contactez votre éditeur pour obtenir la mise à jour du serveur wu-ftpd correspondant à votre distribution.

7 Documentation

- Avis de sécurité SuSE-SA:2001:043 ;
- avis de sécurité Debian DSA-087-1 ;
- avis de sécurité Mandrake MDKSA-2001:090 ;
- site de wu-ftpd :
  http://www.wu-ftpd.org

Gestion détaillée du document

29 novembre 2001 version initiale;

03 décembre 2001 première révision :

- retrait de l'avis RedHat (la version présentée étant encore vulnérable) ;
- mention de la version 2.6.2 (non vulnérable) ;
- ajouts des avis de sécurité Mandrake et Debian.