Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 janvier 2002
N° CERTA-2002-ALE-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation d'une faille de wu-ftpd

Gestion du document

Référence	CERTA-2002-ALE-002
Titre	Exploitation d'une faille de wu-ftpd
Date de la première version	28 janvier 2002
Date de la dernière version	–
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

Compromission du système.

2 Systèmes affectés

Tous les systèmes avec `wu-ftpd` versions 2.6.1 et antérieures, ainsi que certaines versions `Beta` 2.7.0.

3 Résumé

Le CERTA a constaté qu'une faille du serveur `wu-ftpd` récemment découverte est actuellement exploitée afin de compromettre les systèmes.

4 Description

Le serveur `wu-ftpd` est un serveur `ftp` livré avec de très nombreuses distributions Linux, et souvent installé par défaut.

Une faille de ce serveur, rendue publique fin novembre 2001 (voir l'avis CERTA-2001-AVI-153), semble actuellement exploitée pour compromettre les systèmes. Des outils permettant d'exploiter cette vulnérabilité sont en libre circulation sur l'Internet.

L'utilisation de cette vulnérabilité nécessite une authentification préalable, qui peut se faire par le biais du compte `anonymous` ou de tout autre compte.

5 Solution

Désactiver tous les serveurs `ftp` non nécessaires, et filtrer le port 21/tcp au niveau du garde-barrière.

Sur les serveurs `ftp`, même si le compte `anonymous` est désactivé, il est recommandé d'appliquer les correctifs de `wu-ftpd` ou de passer en version 2.6.2 :

ftp://ftp.wu-ftpd.org/pub/wu-ftpd-attic/

6 Documentation

L'avis CERTA-2001-AVI-153 :
http://www.certa.ssi.gouv.fr/site/CERTA-2001-AVI-153/index.html

Gestion détaillée du document

28 janvier 2002 version initiale.