

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de WS\_FTP SERVER

---

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-2002-AVI-170>

---

### Gestion du document

Référence	CERTA-2002-AVI-170
Titre	Vulnérabilité de WS_FTP SERVER
Date de la première version	09 août 2002
Date de la dernière version	–
Source(s)	Avis de sécurité "WS_FTP SITE CPWD buffer overflow vulnerability" de @stake
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.

## 2 Systèmes affectés

WS\_FTP SERVER 3.1.1 pour Windows NT, Windows 2000 et Windows XP.

## 3 Résumé

Une vulnérabilité de type débordement de mémoire permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges du compte SYSTEM.

## 4 Description

WS\_FTP SERVER est un serveur FTP distribué par la société Ipswitch.

Une vulnérabilité est présente dans la routine de changement des mots de passe utilisateur (`site cpwd`). L'exploitation de cette vulnérabilité permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges du compte SYSTEM.

## 5 Contournement provisoire

L'option `Disable Password Change` positionnée au niveau du serveur ftp interdit à l'utilisateur de changer le mot de passe.

## 6 Solution

Appliquer le correctif WS\_FTP SERVER 3.1.2 disponible sur le site de l'éditeur (cf. section documentation).

## 7 Documentation

- Avis de sécurité "WS\_FTP SITE CPWD buffer overflow vulnerability" de @stake :  
<http://www.atstake.com/research/advisories/2002/a080802-1.txt>
- WS\_FTP Server Support Center (Ipswitch) :  
[http://www.ipswitch.com/Support/WS\\_FTP-Server/patch-upgrades.html](http://www.ipswitch.com/Support/WS_FTP-Server/patch-upgrades.html)

## Gestion détaillée du document

09 août 2002 version initiale.