

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-2004-AVI-381>

Gestion du document

Référence	CERTA-2004-AVI-381
Titre	Vulnérabilité dans WS_FTP Server
Date de la première version	01 décembre 2004
Date de la dernière version	–
Source(s)	Liste de diffusion Bugtraq "Multiple buffer overflows in WS_FTP Server" du 29 novembre 2004
Pièce(s) jointe(s)	

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.x ;
- WS_FTP Server 4.x ;
- WS_FTP Server 5.x.

3 Résumé

Plusieurs vulnérabilités présentes dans WS_FTP Server permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sur le système vulnérable.

4 Description

WS_FTP Server est un serveur FTP.

Plusieurs vulnérabilités de type débordement de mémoire ont été découvertes dans les commandes suivantes : SITE, XMKD, MKD et RNFR.

Ces vulnérabilités peuvent être exploitées pour permettre à une personne malveillante d'exécuter du code arbitraire à distance, en appelant les commandes vulnérables avec un argument variable d'environ 768 octets.

5 Contournement provisoire

- Autoriser l'accès aux serveurs vulnérables uniquement aux utilisateurs de confiance ;
- filtrer les requêtes anormalement longues au moyen d'un serveur mandataire proxy FTP.

6 Solution

A ce jour, aucun correctif n'est proposé par l'éditeur. (cf. Documentation)

7 Documentation

- Site Internet de l'éditeur :
<http://www.ipswitch.com>
- Liste de diffusion Bugtraq "Multiple buffer overflows in WS_FTP Server" du 29 novembre 2004 :
<http://www.securityfocus.com/archive/1/382624/2004-11-27/2004-12-03/0>

Gestion détaillée du document

01 décembre 2004 version initiale.