

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ws_ftp

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-2006-AVI-422>

Gestion du document

Référence	CERTA-2006-AVI-422
Titre	Vulnérabilité dans ws_ftp
Date de la première version	04 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité IPSwitch du 14 septembre 2006
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 5.05 et versions antérieures.

3 Résumé

Une vulnérabilité dans WS_FTP Server permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire peut être exploitée en passant des arguments spécialement conçus aux commandes suivantes XCRC, XSHA1 et XMD5. Une personne malveillante pourrait ainsi exécuter du code arbitraire à distance sur le serveur vulnérable.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité IPSwitch du 14 septembre 2006 :
http://ipswitch.com/support/ws_ftp-server/releases/wr505hf1.asp
- Référence CVE CVE-2006-4847 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4847>
- Référence CVE CVE-2006-5000 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5000>
- Référence CVE CVE-2006-5001 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5001>

Gestion détaillée du document

04 octobre 2006 version initiale.