

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité Microsoft (service Serveur)

---

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-443>

---

### Gestion du document

Référence	CERTA-2006-AVI-443
Titre	Vulnérabilité Microsoft (service Serveur)
Date de la première version	11 octobre 2006
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

Déni de service.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professionnel Édition x6 ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 pour les systèmes Itanium et Microsoft Windows ;
- Server 2003 avec SP1 pour les systèmes Itanium ;
- Microsoft Windows Server 2003 Édition x64.

## 3 Résumé

Il existe dans le service Serveur une vulnérabilité pouvant provoquer un déni de service.

## 4 Description

Le service Serveur permet de partager des ressources locales (disques, imprimantes) afin que les autres utilisateurs du réseau puissent y avoir accès. Il permet également une communication par canal nommé (`named pipe`) entre les applications s'exécutant sur différents ordinateurs. Cette vulnérabilité est due au mode de gestion de certains messages réseau. Un attaquant pourrait exploiter cette vulnérabilité en envoyant un paquet réseau spécialement conçu à un ordinateur vulnérable exécutant le service Serveur.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Microsoft MS06-063 du 11 octobre 2006 :  
<http://www.microsoft.com/france/technet/security/bulletin/MS06-063.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS06-063.msp>
- Référence CVE :  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3942>

## Gestion détaillée du document

11 octobre 2006 version initiale.