Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 juin 2006
N° CERTA-2006-AVI-247

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités SMB dans Microsoft Windows

Gestion du document

Référence	CERTA-2006-AVI-247
Titre	Vulnérabilités SMB dans Microsoft Windows
Date de la première version	16 juin 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft du 13 juin 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

- Contournement de la politique de sécurité ;
- déni de service.

2 Systèmes affectés

- Microsoft 2000 Service Pack 4 ;
- Microsoft XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 (incluant les versions x64 Edition et Itanium).

3 Description

Deux vulnérabilités ont été identifiées dans SMB (pour *Server Message Block*), le protocole utilisé par Windows pour rendre accessible des éléments locaux (documents partagés, imprimantes,etc) à d'autres ordinateurs.

- La première concerne le traitement de certaines requêtes SMB, qui n'est pas effectué correctement. Une personne distante peut, après s'être identifiée, envoyer un paquet malveillant exploitant cette vulnérabilité, afin d'élever ses privilèges à ceux de l'administrateur.

– La deuxième concerne des fonctions inclues dans le fichier `mrxsmb.exe`. Il serait possible pour une personne malveillante ayant un code appelant cette librairie de bloquer le processus et par conséquent de créer un déni de service.

4 Solution

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

5 Documentation

– Bulletin de sécurité Microsoft MS06-030 du 13 juin 2006 :
http://www.microsoft.com/france/technet/securite/MS06-030.mspx
http://www.microsoft.com/technet/security/Bulletin/MS06-030.mspx
– Référence CVE CVE-2006-2373 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2373
– Référence CVE CVE-2006-2374 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2374

Gestion détaillée du document

16 juin 2006 version initiale.