



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 juin 2005
N° CERTA-2005-AVI-213-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans SMB de Microsoft

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-2005-AVI-213>

Gestion du document

Référence	CERTA-2005-AVI-213-001
Titre	Vulnérabilité dans SMB de Microsoft
Date de la première version	15 juin 2005
Date de la dernière version	17 juin 2005
Source(s)	Bulletin de sécurité MS05-027
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 à distance ;
- déni de service.

2 Systèmes affectés

- Microsoft Windows 2000 SP3 ;
- Microsoft Windows XP SP1 et SP2 ;
- Microsoft Windows XP édition 64-Bit SP1 (itanium) ;
- Microsoft Windows XP édition 64-Bit version 2003 (itanium) ;
- Microsoft Windows XP Professional édition 64 bits ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 SP1 ;
- Microsoft Windows Server 2003 (itanium) ;
- Microsoft Windows Server 2003 SP1 (itanium) ;

3 Résumé

Une vulnérabilité présente sur le service SMB (Server Message Block) peut être exploitée par un utilisateur mal intentionné pour exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire est présente sur le service SMB. Un utilisateur mal intentionné peut exploiter cette vulnérabilité via une requête SMB malicieusement construite pour réaliser un déni de service ou exécuter du code arbitraire sur la machine 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 Microsoft MS05-027 :
<http://www.microsoft.com/france/technet/securite/ms05-027.msp>
- Référence CVE CAN-2005-1206 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1206>

Gestion détaillée du document

15 juin 2005 version initiale.

17 juin 2005 mise à jour des systèmes affectés (ajout de Microsoft Windows 2000 SP4).