

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans SMB (Service Message Block) 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-2002-AVI-266>

---

### Gestion du document

Référence	CERTA-2002-AVI-266
Titre	Vulnérabilité dans SMB (Service Message Block) de Microsoft
Date de la première version	13 décembre 2002
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

Modification de la politique de groupe.

## 2 Systèmes affectés

- Microsoft Windows 2000 ;
- Microsoft Windows XP.

## 3 Résumé

Une vulnérabilité dans SMB (Service Message Block) de Microsoft permet à un utilisateur local mal intentionné de désactiver l'authentification lors de la négociation d'une session SMB, et de modifier les informations échangées.

## 4 Description

SMB (Service Message Block), initialement conçu comme un protocole de partage de fichiers, est aujourd'hui principalement utilisé pour propager des informations sur la gestion des groupes d'utilisateurs depuis les contrôleurs de domaine vers les systèmes nouvellement connectés.

SMB peut être configuré de sorte que ces informations soient authentifiées par le contrôleur de domaine. En intervenant au moment de la négociation de la session SMB, un utilisateur mal intentionné peut faire en sorte que les données de cette session ne soient pas authentifiées.

## **5 Solution**

Consulter le bulletin de sécurité MS02-070 de Microsoft (voir paragraphe documentation) pour connaître la disponibilité des correctifs.

## **6 Documentation**

Bulletin de sécurité MS02-070 de Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/MS02-070.asp>

## **Gestion détaillée du document**

**13 décembre 2002** version initiale.