



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 juillet 2003
N° CERTA-2003-AVI-105

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de SMB dans Microsoft Windows

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-2003-AVI-105>

Gestion du document

Référence	CERTA-2003-AVI-105
Titre	Vulnérabilité de SMB dans Microsoft Windows
Date de la première version	10 juillet 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #MS03-024 de Microsoft
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

- Microsoft Windows NT Server 4.0 ;
- Microsoft Windows NT Server 4.0, Terminal Server Edition ;
- Microsoft Windows 2000 ;
- Microsoft Windows XP Professional.

3 Résumé

Une vulnérabilité présente dans certaines versions de Microsoft Windows permet à un individu mal intentionné d'exécuter du code arbitraire sur la machine vulnérable.

4 Description

Server Message Block (SMB) est un protocole utilisé pour le partage de ressources sous Windows et pour la communication entre clients à l'aide fichiers spéciaux : les tubes nommés et les *mail slots*.

Une vulnérabilité due à une mauvaise gestion des requêtes client SMB par un serveur permet à un individu mal intentionné possédant un compte valide d'exécuter du code arbitraire à distance.

5 Contournement provisoire

Bloquer les ports 139/TCP et 445/TCP sur le garde-barrière pour empêcher les attaques provenant de l'extérieur du réseau.

6 Solution

Appliquer les correctifs fournis par Microsoft suivant la version du système d'exploitation.

7 Documentation

Bulletin de sécurité #MS03-024 de Microsoft :

http://www.microsoft.com/security/security_bulletins/ms03-024.asp

Référence CVE CAN-2003-0345 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0345>

Gestion détaillée du document

10 juillet 2003 version initiale.