

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité SMB sous 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-2004-ALE-006>

Gestion du document

Référence	CERTA-2004-ALE-006
Titre	Vulnérabilité SMB sous Windows
Date de la première version	28 avril 2004
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 ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Les versions suivantes ont été testées par le CERTA et s'avèrent vulnérables :

- Microsoft Windows 2000 Workstation SP4 ;
- Microsoft Windows XP Professional, XP Professional SP1a.

D'autres versions non testées peuvent également être affectées.

3 Résumé

Un utilisateur mal intentionné mettant à disposition un serveur de fichiers malicieusement construit peut effectuer un déni de service ou réaliser l'exécution de code arbitraire à distance sur une plate-forme cliente vulnérable.

4 Description

Dans la note d'information #322857 publiée en juin 2003, Microsoft indique qu'une faille présente lors de l'accès à un partage de fichiers avec un nom contenant plus de 300 caractères est corrigée dans les derniers Services Packs.

Les tests effectués par le CERTA mettent en évidence que cette vulnérabilité est toujours présente sur les plates-formes Microsoft Windows 2000 et Microsoft Windows XP munies des derniers Services Packs.

En incitant un utilisateur à accéder à un serveur de fichiers partagés habilement configuré, il est possible de forcer l'exécution de code arbitraire à distance sur la plate-forme Windows vulnérable.

5 Contournement provisoire

Dans l'attente de l'application du correctif, désactiver le client pour les réseaux Microsoft.

A défaut, interdire l'accès aux fichiers partagés au niveau des pare-feux (filtrage des ports 139/tcp, 139/udp et 445/tcp).

6 Documentation

Base de connaissances Microsoft #322857 :

<http://support.microsoft.com/default.aspx?kbid=322857>

7 Solution

Le **service pack** SP2 pour Windows XP, et le **service pack** SP4 Update Rollup 1 (Windows 2000) corrigent ce problème. Se référer au site du constructeur pour l'obtention de ces **service pack** (cf. section Documentation)

Gestion détaillée du document

28 avril 2004 version initiale.