

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de mémoire dans le gestionnaire de ressources partagées 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-2002-AVI-185>

Gestion du document

Référence	CERTA-2002-AVI-185
Titre	Débordement de mémoire dans le gestionnaire de ressources partagées sous Windows
Date de la première version	23 août 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS02-045 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 ;
- déni de service.

2 Systèmes affectés

- Windows NT 4.0 Workstation, Server et Terminal Server Edition ;
- Windows 2000 Pro, Server et Advanced Server ;
- Windows XP Pro.

3 Résumé

Un utilisateur mal intentionné peut utiliser un débordement de mémoire dans le gestionnaire des ressources partagées pour effectuer un déni de service, voire exécuter du code arbitraire.

4 Description

Network Share Provider est le gestionnaire de ressources partagées sous Windows. Il utilise un protocole appelé SMB (*Server Message Block*) et permet de partager des ressources telles que des fichiers, imprimantes, ports série, etc.

Un utilisateur mal intentionné peut effectuer un débordement de mémoire sur un serveur de ressources partagées au moyen d'une requête de client SMB habilement construite. Pour effectuer cette attaque l'utilisateur mal intentionné doit être un utilisateur authentifié ou bien utiliser le compte anonyme.

5 Contournement provisoire

- Désactiver le compte anonyme du serveur (ceci n'empêche pas d'utiliser un compte utilisateur authentifié pour effectuer l'attaque).
- Bloquer les ports 139/TCP et 445/TCP sur le garde-barrière pour empêcher les attaques provenant de l'extérieur du réseau.
- Désactiver le serveur Lanman si le système n'est pas un serveur de ressources partagées.

6 Solution

Appliquer le correctif de Microsoft comme indiqué dans le bulletin de sécurité MS02-045 (voir paragraphe documentation).

7 Documentation

Bulletin de sécurité MS02-045 de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/ms02-045.asp>

Gestion détaillée du document

23 août 2002 version initiale.