Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 avril 2002
N° CERTA-2001-AVI-084-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les serveurs RPC sous Windows

Gestion du document

Référence	CERTA-2001-AVI-084-001
Titre	Vulnérabilité dans les serveurs RPC sous Windows
Date de la première version	27 juillet 2001
Date de la dernière version	26 avril 2002
Source(s)	Bulletin Microsoft MS01-041
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.

2 Systèmes affectés

- Microsoft Exchange Server 5.5 ;
- Microsoft Exchange Server 2000 ;
- Microsoft SQL Server 7.0 ;
- Microsoft SQL Server 2000 ;
- Microsoft Windows NT4.0 ;
- Microsoft Windows 2000.

3 Résumé

Une mauvaise interprétation dans la gestion des entrées des serveurs RPC (Remote Procedure Call) peut entraîner un déni de service sur la machine affectée.

4 Description

Le système RPC permet, lors d'utilisation d'applications réparties, d'appeler des fonctions situées sur une machine distante. Lors du dialogue entre une machine serveur et une machine client selon le protocole RPC, les connexions réseaux sont gérées par des « *stubs* » (souches). La souche du système client assure donc la liaison de façon transparente pour l'application utilisée, avec la souche du système serveur.

Lors de la mise en place de plusieurs serveurs RPC, les données provenant des souches ne sont pas systématiquement marquées comme reçues correctement par ces serveurs.

Un utilisateur distant mal intentionné peut, en envoyant des requêtes RPC judicieusement composées, entraîner un encombrement des serveurs RPC pouvant obliger à un redémarrage des machines cibles.

5 Contournement provisoire

Pour se prémunir contre les attaques provenant d'Internet, il convient de bloquer le port 135/TCP au niveau du garde barrière.

6 Solution

Se référer au bulletin de sécurité de Microsoft (voir paragraphe Documentation) pour connaitre la disponibilité des correctifs.

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-041.asp

Gestion détaillée du document

27 juillet 2001 version initiale.
24 avril 2002 seconde version : modification dans la liste des correctifs du bulletin Microsoft.