Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 septembre 2001
N° CERTA-2001-AVI-093

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le serveur RPC sous Windows NT 4.0

Gestion du document

Référence	CERTA-2001-AVI-093
Titre	Vulnérabilité dans le serveur RPC sous Windows NT 4.0
Date de la première version	12 septembre 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-048
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 Windows NT 4.0.

3 Résumé

Une vulnérabilité présente dans le module `RPC endpoint mapper` permet à un utilisateur mal intentionné, par le biais d'un paquet astucieusement construit vers le port 135 de la machine cible, d'engendrer un déni de service sur le service RPC.

4 Description

Le système RPC permet, lors d'utilisation d'applications réparties, d'appeler des fonctions situées sur une machine distante.

RPC emploie le protocole IP (TCP ou UDP) pour communiquer avec ses clients. Un service RPC, disponible sur deux machines différentes, peut employer un port différent pour chacune des machines. Avant le départ d'une session RPC, la machine cliente consulte `RPC endpoint mapper` sur le serveur pour connaître le port utilisé par RPC sur une machine déterminée.

Un paquet malformé envoyé vers le port 135 du module `RPC endpoint mapper` peut faire échouer ce service, rendant tous les services RPC indisponibles.

5 Contournement provisoire

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

6 Solution

Télécharger le correctif sur le site Microsoft :

- Windows NT 4.0 Workstation, Server, Server Enterprise Edition :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32503
- Le correctif pour NT 4.0 Terminal Server Edition n'est actuellement pas disponible sur le site.

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-048.asp

Gestion détaillée du document

12 septembre 2001 version initiale.