



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 octobre 2004
N° CERTA-2004-AVI-333

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la bibliothèque RPC sous Windows NT 4.0

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-AVI-333>

Gestion du document

Référence	CERTA-2004-AVI-333
Titre	Vulnérabilité de la bibliothèque RPC sous Windows NT 4.0
Date de la première version	13 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS04-029 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

- Déni de service ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Microsoft Windows NT Server 4.0 Service Pack 6a ;
- Microsoft Windows NT Terminal Server 4.0 Edition Service Pack 6.

3 Description

Selon Microsoft, une vulnérabilité de type débordement de mémoire affecte la bibliothèque RPC Runtime.

Un utilisateur mal intentionné peut, par l'envoi de messages habilement constitués, lire des parties de la mémoire ou provoquer un déni de service du serveur vulnérable.

4 Contournement provisoire

Filtrer les ports 135/tcp, 139/tcp, 445/tcp, 593/tcp, 135/udp, 137/udp, 138/udp , 445/udp et tout port arbitraire utilisé par un service RPC.

Si le service CIS ou RPC sur HTTP est activé, alors les ports 80/tcp et 443/tcp sont également à filtrer (en tenant compte des serveurs web).

5 Solution

Se référer au bulletin de sécurité de l'éditeur (cf. section Documentation) pour l'obtention des correctifs.

6 Documentation

- Bulletin de sécurité Microsoft MS04-029 du 12 octobre 2004 :
<http://www.microsoft.com/technet/security/bulletin/ms04-029.msp>
- Référence CVE CAN-2004-0569 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0569>

Gestion détaillée du document

13 octobre 2004 version initiale.