Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 mars 2003
N° CERTA-2003-AVI-066

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les RPC sous Windows

Gestion du document

Référence	CERTA-2003-AVI-066
Titre	Vulnérabilité dans les RPC sous Windows
Date de la première version	27 mars 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #MS03-010 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.

2 Systèmes affectés

- Windows NT 4.0 ;
- Windows 2000 ;
- Windows XP.

3 Résumé

Une vulnérabilité a été découverte dans l'implémentation des RPC (Remote Procedure Call) sous Windows.

4 Description

RPC (Remote Procedure Call) est un protocole de type client/serveur utilisé pour l'implémentation d'applications réparties. L'implémentation de ce protocole sous Windows est dérivé de celui de l'OSF (Open Software

Foundation).

Une vulnérabilité a été découverte dans la gestion des messages RPC avec TCP/IP. Celle vulnérabilité affecte le processus `RPC EndPoint Mapper` écoutant sur le port `135`.

Un utilisateur mal intentionné peut exploiter cette faille afin d'effectuer un déni de service sur les services RPC de la machine ou entraîner la perte de certaines fonctions `COM`.

5 Contournement provisoire

Filtrer le port `135/TCP` et `UDP` avec un élément de filtrage en amont.

6 Solution

Appliquer le correctif fourni pour Windows 2000 et XP (cf. Documentation). Aucun correctif n'est disponible pour Windows NT 4.0, il est donc nécessaire de filtrer le port `135/TCP et UDP`.

7 Documentation

Bulletin de sécurité #MS03-010 de Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS03-010.asp

Gestion détaillée du document

27 mars 2003 version initiale.