Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 juillet 2003
N° CERTA-2003-AVI-111

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans l'interface RPC Windows

Gestion du document

Référence	CERTA-2003-AVI-111
Titre	Vulnérabilité dans l'interface RPC Windows
Date de la première version	17 juillet 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité #MS03-026 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.

2 Systèmes affectés

- Microsoft Windows NT 4.0 ;
- Microsoft Windows NT 4.0 Terminal Services Edition ;
- Micorsoft Windows 2000 ;
- Microsoft Windows XP ;
- Microsoft Windows Server 2003.

3 Résumé

Une vulnérabilité a été découverte dans la mise en oeuvre des RPC (Remote Procedure Call) sous Windows.

4 Description

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

Une vulnérabilité a été découverte dans la gestion des messages RPC avec TCP/IP. Cette vulnérabilité affecte l'interface DCOM (Distributed Component Object Model) en écoute sur le port 135.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité afin d'exécuter du code arbitraire à distance avec les privilèges du compte `Local System`.

5 Contournement provisoire

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

6 Solution

Appliquer le correctif fourni par Microsoft suivant la version du système d'exploitation (cf. Documentation).

7 Documentation

Bulletin de sécurité #MS03-026 de Microsoft :
http://www.microsoft.com/security/security_bulletins/ms03-026.asp
Référence CVE CAN-2003-0352 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0352

Gestion détaillée du document

17 juillet 2003 version initiale.