



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 avril 2004
N° CERTA-2004-AVI-127

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de Microsoft RPC/DCOM

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-127>

Gestion du document

Référence	CERTA-2004-AVI-127
Titre	Multiples vulnérabilités de Microsoft RPC/DCOM
Date de la première version	14 avril 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS04-012 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 Workstation 4.0 Service Pack 6a ;
- Microsoft Windows NT Server 4.0 Service Pack 6a ;
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6 ;
- Microsoft Windows 2000 Service Pack 2, Service Pack 3 et Service Pack 4 ;
- Microsoft Windows XP et Microsoft Windows XP Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 64-Bit Edition ;
- Microsoft Windows 98, Microsoft Windows 98 SE et Microsoft Windows Millenium Edition.

3 Résumé

Plusieurs vulnérabilités affectant le service RPC/DCOM de Microsoft permettent l'exécution de code arbitraire à distance.

4 Description

Une vulnérabilité affecte la bibliothèque RPC Runtime. Un utilisateur mal intentionné peut, par l'envoi de messages habilement constitués qui seront traités par cette bibliothèque, exécuter du code arbitraire à distance (référence CVE CAN-2003-0813).

Une vulnérabilité est présente dans le service RPCSS. Un utilisateur mal intentionné peut provoquer l'arrêt brutal de ce service par l'envoi d'un message habilement constitué (référence CVE CAN-2004-0116).

Une vulnérabilité affecte les services CIS (COM Internet Service) et RPC sur HTTP. Un utilisateur mal intentionné peut provoquer l'arrêt brutal de ces services par l'envoi d'un message habilement constitué (référence CVE CAN-2003-0807).

Une vulnérabilité affecte la manière dont les identifiants d'objet COM sont créés. Un utilisateur mal intentionné peut exploiter cette vulnérabilité pour forcer une application à accepter des requêtes de communication (référence CVE CAN-2004-0124).

5 Contournement provisoire

Filtrer les ports 135/tcp, 139/tcp, 445/tcp, 593/tcp, 135/udp, 137/udp, 138/udp et 445/udp. 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).

6 Solution

Appliquer le correctif de Microsoft indiqué dans le bulletin de sécurité MS04-012 (voir Documentation).

7 Documentation

Bulletin de sécurité MS04-012 de Microsoft :

<http://www.microsoft.com/technet/security/bulletin/ms04-012.mspx>

Référence CVE CAN-2003-0813 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0813>

Référence CVE CAN-2004-0116 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0116>

Référence CVE CAN-2003-0807 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0807>

Référence CVE CAN-2004-0124 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0124>

Gestion détaillée du document

14 avril 2004 version initiale.