



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 septembre 2003
N° CERTA-2003-AVI-149-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le service RPCSS sous Windows

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-2003-AVI-149>

Gestion du document

Référence	CERTA-2003-AVI-149-001
Titre	Vulnérabilités dans le service RPCSS sous Windows
Date de la première version	11 septembre 2003
Date de la dernière version	17 septembre 2003
Source(s)	Bulletin Microsoft MS03-039
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 ;
- Déni de service.

2 Systèmes affectés

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

3 Résumé

Trois vulnérabilités ont été découvertes dans le service RPCSS sous Windows.

4 Description

Deux vulnérabilités dans le service Microsoft RPCSS permettent à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance avec les privilèges du compte `Local System`. Ces vulnérabilités affectent l'interface DCOM (Distributed Component Object Model) qui s'appuie sur l'infrastructure RPC.

Une troisième vulnérabilité affectant Microsoft Windows 2000 permet, via l'envoi de paquets judicieusement composés en direction du service RPCSS, de réaliser un déni de service sur la machine cible.

Des programmes permettant d'exploiter cette vulnérabilité sont largement diffusés sur l'Internet.

5 Contournement provisoire

- Filtrer les ports RPC (135 TCP/UDP, 137 UDP, 138 UDP, 139 TCP, 445 TCP/UDP, 593 TCP) avec un élément de filtrage en amont ;
- COM Internet Services est un élément permettant de faire passer des messages RPC par le protocole HTTP. Il est recommandé de désactiver cet élément ou de filtrer les ports 80 et 443 TCP ;
- désactiver l'interface DCOM.

6 Solution

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

7 Documentation

Bulletin de sécurité MS03-039 de Microsoft :

<http://www.microsoft.com/technet/security/bulletin/ms03-039.asp>

Bulletin du CERT CC CA-2003-23 :

<http://www.cert.org/advisories/CA-2003-23.html>

Référence CVE CAN-2003-0715 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0715>

Référence CVE CAN-2003-0528 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0528>

Référence CVE CAN-2003-0605 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0605>

Gestion détaillée du document

11 septembre 2003 version initiale ;

17 septembre 2003 ajout d'informations.