

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Windows RPC

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-2009-AVI-221>

Gestion du document

Référence	CERTA-2009-AVI-221
Titre	Vulnérabilité de Windows RPC
Date de la première version	10 juin 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-026 du 09 juin 2009
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 et 3 ;
- Windows XP Professionnel édition 64 bits Service Pack 2 ;
- Windows Server 2003, toutes architectures (Itanium, 32 et 64 bits), Service Pack 2 ;
- Windows Vista, toutes architectures (32 et 64 bits), tous Services Pack ;
- Windows Server 2008, toutes architectures (Itanium, 32 et 64 bits).

3 Résumé

Une vulnérabilité affectant la fonction d'appel de procédure distante (RPC) de *Microsoft Windows* permet à un individu distant d'élever ses privilèges et d'exécuter du code arbitraire.

4 Description

Une vulnérabilité affectant la mise à jour de l'état du moteur d'ordonnancement de la fonction d'appel de procédure distante (*RPM Marshalling Engine* ou *NDR*) de *Microsoft Windows* permet à un individu distant d'élever ses privilèges et d'exécuter du code arbitraire.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS09-026 du 09 juin 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-026.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-026.msp>
- Référence CVE CVE-2009-0568 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0568>

Gestion détaillée du document

10 juin 2009 version initiale.