Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 mai 2007
N° CERTA-2007-AVI-209

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de l'interface Microsoft DNS RPC

Gestion du document

Référence	CERTA-2007-AVI-209
Titre	Vulnérabilité de l'interface Microsoft DNS RPC
Date de la première version	09 mai 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-029 du 08 mai 2007
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 2000 Service Pack 4 ;
- Microsoft Windows Server 2003, Service Pack 1 et Service Pack 2 (y compris pour les systèmes basés sur Itanium et les éditions x64).

3 Résumé

Une vulnérabilité a été identifiée dans le service serveur de résolution de noms DNS de Microsoft Windows. Celle-ci est exploitable à distance par le réseau, et permet de prendre le contrôle de la machine vulnérable.

4 Description

Une vulnérabilité a été identifiée dans le service serveur de résolution de noms DNS de Microsoft Windows. L'interface de gestion RPC (pour *Remote Procedure Call*) du service serveur DNS ne manipulerait pas correctement certains paquets, pouvant provoquer un débordement de tampon.

Cette vulnérabilité est actuellement exploitée par plusieurs codes malveillants, et a fait l'objet de l'alerte CERTA-2007-ALE-010 le 16 avril 2007.

5 Solution

Se référer au bulletin de sécurité MS07-029 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Alerte CERTA-2007-ALE-010 du 16 avril 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-010/
- Bulletin de sécurité Microsoft MS07-029 du 08 mai 2007 :
  http://www.microsoft.com/france/technet/security/bulletin/MS07-029.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-029.mspx
- Référence CVE CVE-2007-1748 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1748

Gestion détaillée du document

09 mai 2007 version initiale.