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 juin 2006
N° CERTA-2006-AVI-244

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans RRAS de Microsoft Windows

Gestion du document

Référence	CERTA-2006-AVI-244
Titre	Vulnérabilités dans RRAS de Microsoft Windows
Date de la première version	14 juin 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft du 13 juin 2006
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 2000 Service Pack 4 ;
- Microsoft XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 (incluant les versions x64 Edition et Itanium).

3 Description

Des vulnérabilités ont été identifiées dans le service `RRAS` inclu dans plusieurs versions de Microsoft Windows. Le service RAS (pour *Remote Access Service*) est fourni par le système d'exploitation pour offrir aux utilisateurs un moyen de se connecter à d'autres machines via des connexions RNIS (téléphonie) ou X.25. Le service étendu RRAS (pour *Routing and Remote Access Service*) permet aussi de transformer une machine en un routeur.

Le service ne vérifie pas correctement certaines allocations de mémoire. Un utilisateur malveillant peut s'appuyer sur celles-ci pour exécuter du code arbitraire à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité Microsoft MS06-025 du 13 juin 2006 :
  http://www.microsoft.com/france/technet/securite/MS06-025.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS06-025.mspx
- Référence CVE CVE-2006-2370 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2370
- Référence CVE CVE-2006-2371 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2371

Gestion détaillée du document

14 juin 2006 version initiale.