



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 juin 2002  
N° CERTA-2002-AVI-122

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité dans l'annuaire des services RAS et RRAS de 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-2002-AVI-122>

---

### Gestion du document

Référence	CERTA-2002-AVI-122
Titre	Vulnérabilité dans l'annuaire des services RAS et RRAS de Windows
Date de la première version	13 juin 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS02-029 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

- Elévation de privilèges ;
- déni de service ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

- Microsoft Windows NT 4.0 ;
- Microsoft Windows NT 4.0 Terminal Server Edition ;
- Microsoft Windows 2000 ;
- Microsoft Windows XP ;
- Microsoft Routing and Remote Access Server.

## 3 Résumé

Un individu mal intentionné peut exécuter du code arbitraire à distance en exploitant une vulnérabilité présente dans l'annuaire des services RAS et RRAS.

## **4 Description**

Le service RAS (Remote Access Service) permet d'effectuer des connexions distantes par des lignes téléphoniques. Ce service est fourni en natif dans Windows NT 4.0, 2000 et XP, et peut être délivré séparément comme RRAS (Routing and Remote Access Server) sous Windows NT 4.0. Ces services possèdent un annuaire permettant de stocker des informations sur des numéros d'appel, de sécurité ou de configuration réseau.

Une vulnérabilité présente dans cet annuaire permet d'effectuer un déni de service, ou bien d'exécuter du code arbitraire avec les privilèges du compte LocalSystem.

## **5 Solution**

Se référer au bulletin de sécurité MS02-029 de Microsoft (cf. Documentation) pour connaître la disponibilité des correctifs disponibles.

## **6 Documentation**

Bulletin de sécurité MS02-029 de Microsoft :

<http://www.microsoft.com/technet/security/bulletin/MS02-029.asp>

## **Gestion détaillée du document**

**13 juin 2002** version initiale.