



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 10 août 2005  
N° CERTA-2005-AVI-304

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du protocole RDP de Microsoft

---

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-2005-AVI-304>

---

### Gestion du document

Référence	CERTA-2005-AVI-304
Titre	Vulnérabilité du protocole RDP de Microsoft
Date de la première version	10 août 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-041 du 09 août 2005
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

Déni de service.

## 2 Systèmes affectés

- Microsoft Windows 2000 Server Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 pour systèmes Itanium et Microsoft Windows Server 2003 pour systèmes Itanium Service Pack 1 ;
- Microsoft Windows Server 2003 x64 Edition.

## 3 Résumé

Une vulnérabilité dans Remote Desktop Protocol permet de réaliser un déni de service.

## **4 Description**

Le protocole RDP (Remote Desktop Protocol) permet à un utilisateur d'établir une session virtuelle graphique vers une autre machine.

Un utilisateur mal intentionné peut, par le biais d'un message RDP malicieusement constitué, provoquer un arrêt du système vulnérable.

## **5 Contournement provisoire**

Filtrer le port 3389/tcp au niveau du pare-feu.

## **6 Solution**

Appliquer le correctif tel qu'indiqué dans le bulletin de sécurité Microsoft MS05-041 (voir Documentation).

## **7 Documentation**

- Bulletin de sécurité Microsoft MS05-041 du 09 août 2005 :  
<http://www.microsoft.com/technet/security/bulletin/MS05-041.msp>
- Référence CVE CAN-2005-1218 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1218>

## **Gestion détaillée du document**

**10 août 2005** version initiale.