

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le client Remote Desktop 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-2011-AVI-142>

---

### Gestion du document

Référence	CERTA-2011-AVI-142
Titre	Vulnérabilité dans le client Remote Desktop de Windows
Date de la première version	09 mars 2011
Date de la dernière version	–
Source(s)	Alerte TA05-023A de l'US-CERT
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

Systèmes affectés avec Remote Desktop Connection 5.2 :

- Windows XP Service Pack 3 Remote Desktop Connection 5.2 Client.

Systèmes affectés avec Remote Desktop Connection 6.1 :

- Windows XP Service Pack 3 Remote Desktop Connection 6.1 Client ;
- Windows XP Professional x64 Edition Service Pack 2 Remote Desktop Connection 6.0 Client ;
- Windows Server 2003 Service Pack 2 Remote Desktop Connection 6.0 Client ;
- Windows Server 2003 Service Pack 2 Remote Desktop Connection 6.0 Client Multilingual User Interface (MUI) ;
- Windows Server 2003 x64 Edition Service Pack 2 Remote Desktop Connection 6.0 Client ;
- Windows Vista Service Pack 1 and Windows Vista Service Pack 2 Remote Desktop Connection 6.1 Client ;
- Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2 Remote Desktop Connection 6.1 Client ;

- Windows Server 2008 for 32-bit Systems and Windows Server 2008 for 32-bit Systems Service Pack 2 Remote Desktop Connection 6.1 Client ;
- Windows Server 2008 for x64-based Systems and Windows Server 2008 for x64-based Systems Service Pack 2 Remote Desktop Connection 6.1 Client ;
- Windows Server 2008 for Itanium-based Systems and Windows Server 2008 for Itanium-based Systems Service Pack 2 Remote Desktop Connection 6.1 Client.

Systèmes affectés avec Remote Desktop Connection 7.0 :

- Windows XP Service Pack 3 Remote Desktop Connection 7.0 Client ;
- Windows Vista Service Pack 1 and Windows Vista Service Pack 2 Remote Desktop Connection 7.0 Client ;
- Windows Vista x64 Edition Service Pack 1 and Windows Vista x64 Edition Service Pack 2 Remote Desktop Connection 7.0 Client ;
- Windows 7 for 32-bit Systems Remote Desktop Connection 7.0 Client ;
- Windows 7 for x64-based Systems Remote Desktop Connection 7.0 Client ;
- Windows Server 2008 R2 for x64-based Systems Remote Desktop Connection 7.0 Client ;
- Windows Server 2008 R2 for Itanium-based Systems Remote Desktop Connection 7.0 Client.

### **3 Résumé**

Une vulnérabilité présente dans le client Remote Desktop Connection permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

### **4 Description**

Une vulnérabilité causée par un manque de contrôle lors du chargement de bibliothèques de liens dynamiques permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

### **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 MS11-017 du 08 mars 2011 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-017.mspx>  
<http://www.microsoft.com/technet/security/Bulletin/MS11-017.mspx>
- Référence CVE CVE-2011-0029 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0029>

## **Gestion détaillée du document**

**09 mars 2011** version initiale.