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 2012
N° CERTA-2012-AVI-320

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Vulnérabilité dans Windows Remote Desktop Protocol



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2012-AVI-320 |
| Titre | Vulnérabilité dans Windows Remote Desktop Protocol |
| Date de la première version | 13 juin 2012 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Microsoft MS12-036 du 12 juin 2012 |
| 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

- Windows XP Service Pack 3 ;
- Windows XP Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 SP2 pour les systèmes Itanium ;
- Windows Vista Service Pack 2 ;
- Windows Vista x64 Edition Service Pack 2 ;
- Windows Server 2008 32-bit Service Pack 2 ;
- Windows Server 2008 x64 Service Pack 2 ;
- Windows Server 2008 Itanium Service Pack 2 ;
- Windows 7 32-bit ;
- Windows 7 32-bit Service Pack 1 ;
- Windows 7 x64 ;

- Windows 7 x64 Service Pack 1 ;
- Windows Server 2008 R2 x64 ;
- Windows Server 2008 R2 x64 Service Pack 1 ;
- Windows Server 2008 R2 Itanium ;
- Windows Server 2008 R2 Itanium Service Pack 1.

# 3 Résumé

Une vulnérabilité a été corrigée dans *Microsoft Windows Remote Desktop Protocol*. Elle concerne l'accès à un objet effacé ou mal initialisé, un attaquant peut l'utiliser 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 MS12-036 du 12 juin 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/MS12-036
  http://technet.microsoft.com/en-us/security/bulletin/MS12-036
- Référence CVE CVE-2012-0173 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0173

# Gestion détaillée du document

**13 juin 2012** version initiale.