

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le composant de traitement des fichiers dans 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-2012-AVI-721>

---

### Gestion du document

Référence	CERTA-2012-AVI-721
Titre	Vulnérabilité dans le composant de traitement des fichiers dans Windows
Date de la première version	12 décembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-081 du 11 décembre 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

- Microsoft Windows Server 2003 Service Pack 2
- Microsoft Windows Server 2003 Itanium Service Pack 2
- Microsoft Windows Server 2003 x64 Edition Service Pack 2
- Microsoft Windows XP Media Center Edition 2005 Service Pack 3
- Microsoft Windows XP Professional x64 Edition Service Pack 2
- Microsoft Windows XP Service Pack 3
- Microsoft Windows XP Tablet PC Edition 2005 Service Pack 3
- Windows 7 32-bit
- Windows 7 32-bit Service Pack 1
- Windows 7 x64
- Windows 7 x64 Service Pack 1
- Windows Embedded Standard 7 32-bit
- Windows Embedded Standard 7 x64

- Windows Server 2008 R2 Itanium
- Windows Server 2008 R2 Itanium Service Pack 1
- Windows Server 2008 R2 x64
- Windows Server 2008 R2 x64 Service Pack 1
- Windows Server 2008 32-bit Service Pack 2
- Windows Server 2008 Itanium Service Pack 2
- Windows Server 2008 x64 Service Pack 2
- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 2

### **3 Résumé**

Une vulnérabilité a été corrigée dans le composant de traitement des fichiers dans *Windows*. Elle permet à un attaquant d'exécuter du code arbitraire à distance au moyen d'un nom de fichier ou dossier spécialement conçu.

### **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 MS12-081 du 11 décembre 2012 :  
<http://technet.microsoft.com/security/bulletin/ms12-081>
- Référence CVE CVE-2012-4774  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-4774>

## **Gestion détaillée du document**

**12 décembre 2012** version initiale.