

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le noyau 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-444>

---

### Gestion du document

Référence	CERTA-2011-AVI-444
Titre	Vulnérabilité dans le noyau Windows
Date de la première version	10 août 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-068 du 09 août 2011
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 à distance.

## 2 Systèmes affectés

- Windows Vista Service Pack 2 ;
- Windows Vista Edition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Windows 7 pour systèmes 32 bits et Windows 7 pour systèmes 32 bits Service Pack 1 ;
- Windows 7 pour systèmes x64 et Windows 7 pour systèmes x64 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes x64 et Windows Server 2008 R2 pour systèmes x64 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes Itanium et Windows Server 2008 R2 pour systèmes Itanium Service Pack 1 ;
- les installations de Windows Server 2008 en option Server Core ne sont pas concernées.

### **3 Résumé**

Une vulnérabilité dans le noyau de Microsoft Windows permet à un attaquant de générer un déni de service.

### **4 Description**

Une vulnérabilité dans le noyau de Microsoft Windows peut être exploitée par un attaquant pour générer un déni de service. Un utilisateur doit naviguer dans un partage réseau où l'attaquant a placé un fichier spécialement conçu pour activer cette vulnérabilité et forcer le redémarrage du système de l'utilisateur.

### **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 MS11-068 du 09 août 2011 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-068.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS11-068.msp>
- Référence CVE CVE-2011-1971 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1971>

### **Gestion détaillée du document**

**10 août 2011** version initiale.