

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le processeur de scripts Unicode sous Microsoft 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-2010-AVI-432>

---

### Gestion du document

Référence	CERTA-2010-AVI-432
Titre	Vulnérabilité dans le processeur de scripts Unicode sous Microsoft Windows
Date de la première version	15 septembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft ms10-063 du 14 septembre 2010
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 Professionnel Édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Édition x64 Service Pack 2 ;
- Windows Server 2003 avec SP2 pour systèmes Itanium ;
- Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Windows Vista Édition x64 Service Pack 1 et Windows Vista Édition x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes 32 bits et Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2 ;
- Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium Service Pack 2 ;
- Microsoft Office XP Service Pack 3 ;
- Microsoft Office 2003 Service Pack 3 ;
- Microsoft Office 2007 Service Pack 2.

### **3 Résumé**

Une vulnérabilité dans le processeur de scripts `Unicode` dans Microsoft Windows permet l'exécution de code arbitraire à distance.

### **4 Description**

Une vulnérabilité due à traitement incorrect de certaines polices par Microsoft Windows et Microsoft Office 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 MS10-063 du 14 septembre 2010 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-063.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS10-063.msp>
- Référence CVE CVE-2010-2738 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2738>

### **Gestion détaillée du document**

**15 septembre 2010** version initiale.