

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Microsoft Internet Explorer

---

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-2005-AVI-396>

---

### Gestion du document

Référence	CERTA-2005-AVI-396
Titre	Vulnérabilité de Microsoft Internet Explorer
Date de la première version	12 octobre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS05-052 du 11 octobre 2005
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

- Internet Explorer 5.01 Service Pack 4 sur Microsoft Windows 2000 Service Pack 4 ;
- Internet Explorer 6 Service Pack 1 sur Microsoft Windows 2000 Service Pack 4 ou sur Microsoft Windows XP Service Pack 1 ;
- Internet Explorer 6 pour Microsoft Windows XP Service Pack 2 ;
- Internet Explorer 6 pour Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Internet Explorer 6 pour Microsoft Windows Server 2003 pour Systèmes Itanium et Microsoft Windows Server 2003 Service Pack 1 pour Systèmes Itanium ;
- Internet Explorer 6 pour Microsoft Windows Server 2003 Edition x64 ;
- Internet Explorer 6 pour Microsoft Windows XP Professional Edition x64 ;
- Internet Explorer 5.5 Service Pack 2 pour Microsoft Windows Millennium Edition.

### 3 Résumé

Une vulnérabilité dans Microsoft Internet Explorer permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire à distance.

### 4 Description

Il est possible, via Internet Explorer, d'appeler des objets DCOM (Distributed Component Object Model) fournis par la bibliothèque `msdds.dll` (Microsoft DDS Library Shape Control). Une vulnérabilité dans cette bibliothèque (cf. CERTA-2005-ALE-008) permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance par le biais d'un site web malicieusement construit.

### 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention de correctifs (cf. Documentation).

### 6 Documentation

- Site de l'éditeur :  
<http://www.microsoft.com>
- Bulletin de sécurité Microsoft MS05-052 du 11 octobre 2005 :  
<http://www.microsoft.com/technet/security/Bulletin/MS05-052.msp>
- Bulletin d'alerte CERTA-2005-ALE-008 du 19 août 2005 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-ALE-008/CERTA-2005-ALE-008.html>
- Référence CVE CAN-2005-2127 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2127>

### Gestion détaillée du document

12 octobre 2005 version initiale.