



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 19 août 2005  
N° CERTA-2005-ALE-008

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Possible vulnérabilité de la bibliothèque msdds.dll

---

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-ALE-008>

---

### Gestion du document

Référence	CERTA-2005-ALE-008
Titre	Possible vulnérabilité de la bibliothèque msdds.dll
Date de la première version	19 août 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft 906267 du 18 août 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

Systèmes Windows avec la bibliothèque msdds.dll (version 7.0.9064.9112) installée.

Dans ce contexte, les logiciels affectés sont :

- 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 Microsoft Windows XP Service Pack 1 ;
- Internet Explorer 6 sur Microsoft Windows XP Service Pack 2 ;
- Internet Explorer 6 Service Pack 1 sur Microsoft Windows XP 64-Bit Edition Service Pack 1 (Itanium) ;
- Internet Explorer 6 sur Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Internet Explorer 6 sur Microsoft Windows Server 2003 pour systèmes Itanium, Microsoft Windows Server 2003 Service Pack 1 pour systèmes Itanium, Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium), Microsoft Windows Server 2003 x64 Edition et Microsoft Windows XP Professional x64 Edition ;
- Internet Explorer 5.5 Service Pack 2 sur Microsoft Windows Millennium Edition ;

- Internet Explorer 6 Service Pack 1 sur Microsoft Windows 98, Microsoft Windows 98 SE et Microsoft Windows Millennium Edition.

Les autres versions de `msdds.dll` peuvent être vulnérables.

### 3 Résumé

Une vulnérabilité dans la bibliothèque `msdds.dll` permettrait l'exécution de code arbitraire à distance via Internet Explorer.

### 4 Description

La bibliothèque `msdds.dll` (Microsoft DDS Library Shape Control) est un objet COM qui fournit des formes préconstruites pour DDS Designer Surfaces. Cet objet COM est utilisé par des composants tels que Visual Studio Database Diagramming pour permettre de visualiser des objets de bases de données.

Cette bibliothèque n'est pas installée par défaut. Elle peut en revanche être installée avec certains logiciels comme Microsoft Visual Studio .NET 2002, Microsoft Visual Studio .NET 2003, Microsoft Office Professional 2003 ou Microsoft Office XP (liste non exhaustive). La bibliothèque `msdds.dll` n'a pas été conçue pour être utilisée par Internet Explorer, même si cela reste possible. Son usage avec Internet Explorer n'est pas considéré comme sûr.

Une vulnérabilité dans la bibliothèque `msdds.dll` permettrait, via Internet Explorer et au moyen de pages web malicieusement constituées, d'exécuter du code arbitraire à distance.

Un outil permettant de créer des pages web afin d'exploiter cette vulnérabilité est disponible sur l'Internet.

Il n'existe pas de correctif pour le moment.

### 5 Contournement provisoire

- Désactiver les contrôles ActiveX ;
- positionner le `kill bit` dans la base de registre pour le CLSID `EC444CB6-3E7E-4865-B1C3-0DE72EF39B3F` afin d'empêcher l'utilisation de la bibliothèque `msdds.dll` par Internet Explorer (cette mesure n'aura aucun effet secondaire) ;
- désactiver la bibliothèque `msdds.dll` dans le registre avec la commande (cette action peut provoquer des dysfonctionnements au niveau de certaines applications) :  
`regsvr32 /u Msdds.dll`
- modifier les listes de contrôle d'accès (ACL) du fichier `msdds.dll` avec la commande :  
`cacls %windir%\system32\Msdds.dll /d everyone`

### 6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (voir avis CERTA-2005-AVI-396).

### 7 Documentation

- Bulletin de sécurité Microsoft 906267 du 18 août 2005 :  
<http://www.microsoft.com/technet/security/advisory/906267.msp>
- Avis CERTA-2005-AVI-396 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-396/CERTA-2005-AVI-396.html>

## Gestion détaillée du document

**19 août 2005** version initiale.

**12 avril 2006** ajout de la section Solution et mise à jour de la section Documentation.