

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Microsoft Data Access Components

---

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-010>

---

### Gestion du document

Référence	CERTA-2011-AVI-010
Titre	Vulnérabilités dans Microsoft Data Access Components
Date de la première version	12 janvier 2011
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS11-002 du 11 janvier 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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

Microsoft Data Access Components sur les systèmes suivants :

- 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 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 ;
- Windows 7 pour systèmes 32 bits ;
- Windows 7 pour systèmes x64 ;

- Windows Server 2008 R2 pour systèmes x64 ;
- Windows Server 2008 R2 pour systèmes Itanium.

### **3 Résumé**

Des vulnérabilités dans Microsoft Data Access Components (MDAC) pourraient permettre l'exécution de code arbitraire à distance.

### **4 Description**

Deux vulnérabilités dans Microsoft Data Access Components (MDAC) pourraient permettre à une personne malintentionnée d'exécuter du code arbitraire sur le poste d'un client vulnérable au moyen d'une page Web spécialement conçue.

### **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 MS11-002 du 11 janvier 2011 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-002.mspx>  
<http://www.microsoft.com/technet/security/Bulletin/MS11-002.mspx>
- Référence CVE CVE-2011-0026 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0026>
- Référence CVE CVE-2011-0027 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0027>

### **Gestion détaillée du document**

**12 janvier 2011** version initiale.