



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 09 juin 2010  
N° CERTA-2010-AVI-246

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans certains contrôles ActiveX

---

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-246>

---

### Gestion du document

Référence	CERTA-2010-AVI-246
Titre	Vulnérabilité dans certains contrôles ActiveX
Date de la première version	09 juin 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-034 du 20 juin 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

- Microsoft Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 et 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 ;
- 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

Deux vulnérabilités découvertes dans les contrôles ActiveX permettent à un utilisateur malintentionné d'exécuter du code arbitraire à distance.

### 4 Description

Deux vulnérabilités ont été corrigées dans le contrôle ActiveX *Microsoft Data Analyzer* (CVE-2010-0252) et dans Microsoft Internet Explorer 8 *Developer Tools* (CVE-2010-0811). Ces vulnérabilités peuvent être exploitées par une personne malveillante afin d'exécuter du code arbitraire à distance au moyen d'un site web ou d'un document Microsoft Office spécialement construits.

### 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 MS10-034 du 08 juin 2010 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-034.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS10-034.msp>
- Référence CVE CVE-2010-0252 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0252>
- Référence CVE CVE-2010-0811 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0811>

### Gestion détaillée du document

**09 juin 2010** version initiale.