



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 avril 2011  
N° CERTA-2011-AVI-210

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans des contrôles ActiveX de 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-2011-AVI-210>

---

### Gestion du document

Référence	CERTA-2011-AVI-210
Titre	Multiples vulnérabilités dans des contrôles ActiveX de Microsoft Windows
Date de la première version	13 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-027 du 12 avril 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

- 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 32 bits Service Pack 1 ;

- Windows 7 pour systèmes x64 ;
- Windows 7 pour systèmes x64 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes x64 ;
- Windows Server 2008 R2 pour systèmes x64 Service Pack 1 ;
- Windows Server 2008 R2 pour systèmes Itanium ;
- Windows Server 2008 R2 pour systèmes Itanium Service Pack 1.

### 3 Résumé

Plusieurs vulnérabilités dans certains contrôles *ActiveX* de Microsoft Windows permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

### 4 Description

Plusieurs vulnérabilités dans des contrôles *ActiveX* de Microsoft Windows ont été découvertes :

- une vulnérabilité dans le contrôle *ActiveX* des outils de développement Microsoft Internet Explorer 8 permet à une personne distante malintentionnée d'exécuter du code arbitraire ;
- une vulnérabilité dans le contrôle *ActiveX* Microsoft *WMITools* permet à une personne distante malintentionnée d'exécuter du code arbitraire ;
- une vulnérabilité dans le contrôle *ActiveX* de Microsoft Windows Messenger permet à une personne distante malintentionnée d'exécuter du code arbitraire.

### 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 MS11-027 du 12 avril 2011 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-027.aspx>  
<http://www.microsoft.com/technet/security/Bulletin/MS11-027.aspx>
- Référence CVE CVE-2010-0811 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0811>
- Référence CVE CVE-2010-3973 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3973>
- Référence CVE CVE-2011-1243 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1243>

### Gestion détaillée du document

13 avril 2011 version initiale.