

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans des composants 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-2007-AVI-085>

---

### Gestion du document

Référence	CERTA-2007-AVI-085
Titre	Vulnérabilités dans des composants ActiveX de Microsoft Windows
Date de la première version	14 février 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité Microsoft MS07-008 et MS07-009 du 13 février 2007
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 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows Serveur 2003, versions x86 et Itanium.

## 3 Résumé

Une vulnérabilité, permettant l'exécution de code arbitraire à distance, existe dans 2 composants ActiveX, Microsoft Data Access Components et Microsoft HTML Help, de Microsoft Windows.

## 4 Description

Microsoft HTML Help (hhctrl.ocx) est un composant ActiveX permettant l'affichage des fichiers d'aide au format HTML. Une personne malveillante peut exploiter la vulnérabilité présente dans ce composant

ActiveX afin d'exécuter du code arbitraire à distance par le biais d'une page web au format HTML spécialement conçue.

Microsoft Data Access Components (MDAC) est un regroupement de technologies Microsoft facilitant l'accès aux données. Une vulnérabilité présente dans le contrôle ActiveX `ADODB.Connection` permet à une personne malveillante d'exécuter du code arbitraire à distance par le biais d'un appel spécialement conçu d'une méthode de ce contrôle ActiveX.

## 5 Solution

Se référer aux bulletins de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Microsoft MS07-008 du 13 février 2007 :  
<http://www.microsoft.com/france/technet/security/bulletin/MS07-008.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-008.msp>
- Bulletin de sécurité Microsoft MS07-009 du 13 février 2007 :  
<http://www.microsoft.com/france/technet/security/bulletin/MS07-009.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-009.msp>
- Référence CVE CVE-2007-0214 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0214>
- Référence CVE CVE-2006-5559 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5559>

## Gestion détaillée du document

14 février 2007 version initiale.