

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft OLE Automation

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-2008-AVI-073>

Gestion du document

Référence	CERTA-2008-AVI-073
Titre	Vulnérabilité dans Microsoft OLE Automation
Date de la première version	13 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-008 du 12 février 2008
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 2000 Service Pack 4 ;
- Windows XP Service Pack 2 ;
- Windows XP Professionnel Edition x64 ;
- Windows XP Professionnel Edition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 1 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Edition x64 ;
- Windows Server 2003 Edition x64 Service Pack 2 ;
- Windows Server 2003 pour les systèmes Itanium (SP1 et SP2) ;
- Windows Vista ;
- Windows Vista Edition x64 ;
- Microsoft Office 2004 pour Mac ;
- Microsoft Visual Basic 6.0 Service Pack 6.

3 Résumé

Une vulnérabilité a été identifiée dans OLE Automation de Microsoft. Celle-ci pourrait être exploitée par une personne malveillante distante via une page Web spécialement construite, pour exécuter des commandes sur le poste vulnérable, avec les droits de l'utilisateur.

4 Description

Une vulnérabilité a été identifiée dans OLE Automation de Microsoft. Il s'agit d'un protocole de Windows utilisé par une application pour échanger des données ou contrôler une autre application. Des requêtes particulières lors de l'utilisation du service pourraient provoquer une corruption de la mémoire.

Cette vulnérabilité pourrait être exploitée par une personne malveillante distante via une page Web spécialement construite, pour exécuter des commandes sur le poste vulnérable, avec les droits de l'utilisateur.

5 Solution

Se référer au bulletin de sécurité MS08-008 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-008 du 12 février 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-008.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-008.msp>
- Référence CVE CVE-2007-0065 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0065>

Gestion détaillée du document

13 février 2008 version initiale.