

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Microsoft Office

---

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-205>

---

### Gestion du document

Référence	CERTA-2007-AVI-205
Titre	Vulnérabilité dans Microsoft Office
Date de la première version	09 mai 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-025 du 08 mai 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 Office 2000 Service Pack 3 ;
- Microsoft Office XP Service Pack 3 ;
- Microsoft Office 2003 Service Pack 2 ;
- Microsoft Office 2007 ;
- Microsoft Office 2004 pour Mac.

## 3 Résumé

Une vulnérabilité a été identifiée dans la bibliothèque `ms0.dll` commune aux applications de la suite bureautique Microsoft Office. L'exploitation de cette dernière permettrait à une personne malveillante d'exécuter du code arbitraire sur le système.

## 4 Description

Une vulnérabilité a été identifiée dans la bibliothèque `ms0.dll` commune aux applications de la suite bureautique Microsoft Office.

Certains objets de dessin ne seraient pas correctement manipulés, pouvant provoquer un débordement de mémoire. Une personne malveillante pourrait ainsi construire un document Office contenant un tel objet non valide afin d'exécuter du code arbitraire sur le système vulnérable.

## 5 Solution

Se référer au bulletin de sécurité MS07-025 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Microsoft MS07-025 du 08 mai 2007 :  
<http://www.microsoft.com/france/technet/security/bulletin/MS07-025.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-025.msp>
- Référence CVE CVE-2007-1747 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1747>

## Gestion détaillée du document

**09 mai 2007** version initiale.