



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 septembre 2006  
N° CERTA-2006-AVI-389

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Microsoft Publisher

---

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-2006-AVI-389>

---

### Gestion du document

Référence	CERTA-2006-AVI-389
Titre	Vulnérabilité dans Microsoft Publisher
Date de la première version	13 septembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-054 du 12 septembre 2006
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

- Office Publisher 2000 fourni dans la suite Microsoft Office 2000 Service Pack 3 ;
- Office Publisher 2002 fourni dans la suite Microsoft Office XP Service Pack 3 ;
- Office Publisher 2003 fourni dans la suite Microsoft Office 2003 Service Pack 1 et Service Pack 2.

## 3 Résumé

Une vulnérabilité a été identifiée dans certaines versions de l'application Microsoft Publisher. Une personne malveillante pourrait construire un fichier exploitant cette vulnérabilité, afin d'exécuter du code arbitraire sur le système où le document sera ouvert.

## 4 Description

Publisher est une application fournie par Microsoft servant à la publication de documents (logiciel PAO, pour *publication assistée par ordinateur*).

Une vulnérabilité a été identifiée dans ce dernier. Il ne contrôlerait pas de manière correcte certaines chaînes de caractères malformées dans des fichiers au format `.pub`.

Une personne malveillante pourrait construire un fichier exploitant cette vulnérabilité, afin d'exécuter du code arbitraire sur le système où le document sera ouvert.

## 5 Solution

Se référer au bulletin de sécurité MS06-054 de Microsoft pour l'application des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Microsoft MS06-054 du :  
<http://www.microsoft.com/france/technet/security/bulletin/2006/MS06-054.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS06-054.msp>
- Référence CVE CVE-2006-0001 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0001>

## Gestion détaillée du document

13 septembre version initiale.