



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 mai 2008  
N° CERTA-2008-AVI-243

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-2008-AVI-243>

---

### Gestion du document

Référence	CERTA-2008-AVI-243
Titre	Vulnérabilité dans Microsoft Publisher
Date de la première version	14 mai 2008
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS08-027 du 13 mai 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

- Microsoft Publisher 2000 service pack 3 ;
- Microsoft Publisher 2002 service pack 3 ;
- Microsoft Publisher 2003 service pack 2 et service pack 3 ;
- Microsoft Publisher 2007 et 2007 service pack 1.

## 3 Résumé

Une vulnérabilité présente dans Microsoft Publisher permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

## 4 Description

Un défaut de traitement par Publisher des en-têtes des données est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance avec les droits de l'utilisateur du système vulnérable.

## **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 MS08-027 du 13 mai 2008 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-027.msp#>  
<http://www.microsoft.com/technet/security/Bulletin/MS08-027.msp#>
- Référence CVE CVE-2008-0119 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0119>

## **Gestion détaillée du document**

**14 mai 2008** version initiale.