



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 août 2008  
N° CERTA-2008-AVI-411

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilité de Microsoft PowerPoint

---

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-411>

---

### Gestion du document

Référence	CERTA-2008-AVI-411
Titre	Multiples vulnérabilité de Microsoft PowerPoint
Date de la première version	13 août 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-051 du 12 août 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 PowerPoint 2000 Service Pack 3 ;
- Microsoft PowerPoint 2002 Service Pack 3 ;
- Microsoft PowerPoint 2003 Service Pack 2 ;
- Microsoft PowerPoint 2003 Service Pack 3 ;
- Microsoft PowerPoint 2007 Service Pack 2 ;
- Microsoft PowerPoint 2007 Service Pack 3 ;
- Microsoft Office PowerPoint Viewer 2003 ;
- Microsoft Office 2004 pour Mac.

## 3 Résumé

Plusieurs vulnérabilités ont été découvertes dans Microsoft PowerPoint. L'exploitation de ces vulnérabilités permet d'exécuter du code arbitraire à distance.

## 4 Description

Trois vulnérabilités ont été découvertes dans les différentes versions du logiciel bureautique Microsoft PowerPoint :

- la première vulnérabilité est due à une erreur lors d'une allocation mémoire par le logiciel Microsoft PowerPoint Viewer 2003. Cette vulnérabilité peut être exploitée afin d'exécuter du code arbitraire à distance via un document PowerPoint spécialement construit ;
- la deuxième vulnérabilité est liée à la manière dont Microsoft PowerPoint Viewer 2003 calcule la taille de la mémoire à allouer. Cette vulnérabilité peut être exploitée afin d'exécuter du code arbitraire à distance via un document PowerPoint spécialement construit ;
- la troisième vulnérabilité résulte d'un débordement de mémoire dans le traitement des documents PowerPoint par les différentes versions du logiciel Microsoft PowerPoint. Cette vulnérabilité peut être exploitée afin d'exécuter du code arbitraire à distance via un document PowerPoint spécialement construit.

## 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 MS08-051 du 12 août 2008 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-051.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS08-051.msp>
- Référence CVE CVE-2008-0120 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0120>
- Référence CVE CVE-2008-0121 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0121>
- Référence CVE CVE-2008-1455 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1455>

## Gestion détaillée du document

13 août 2008 version initiale.