

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans 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-2009-AVI-185>

---

### Gestion du document

Référence	CERTA-2009-AVI-185
Titre	Multiples vulnérabilités dans Microsoft PowerPoint
Date de la première version	13 mai 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-017 du 12 mai 2009
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 PowerPoint 2000 Service Pack 3 ;
- Microsoft Office PowerPoint 2002 Service Pack 3 ;
- Microsoft Office PowerPoint 2003 Service Pack 3 ;
- Microsoft Office PowerPoint 2007 Service Pack 1 ;
- Microsoft Office PowerPoint 2007 Service Pack 2 ;
- Microsoft Office 2004 pour Mac ;
- Microsoft Office 2008 pour Mac ;
- Convertisseur de formats de fichier Open XML pour Mac ;
- PowerPoint Viewer 2003 ;
- PowerPoint Viewer 2007 Service Pack 1 ;
- PowerPoint Viewer 2007 Service Pack 2 ;
- Pack de compatibilité Office pour les formats de fichier Word, Excel et PowerPoint 2007 Service Pack 1 ;
- Pack de compatibilité Office pour les formats de fichier Word, Excel et PowerPoint 2007 Service Pack 2 ;

- Microsoft Works 8.5 ;
- Microsoft Works 9.0.

### 3 Résumé

Plusieurs vulnérabilités dans *Microsoft Office PowerPoint* permettant l'exécution de code arbitraire à distance ont été corrigées.

### 4 Description

De multiples vulnérabilités dans *Microsoft Office PowerPoint* permettent à une personne malintentionnée d'exécuter du code arbitraire à distance au moyen d'un fichier spécialement conçu.

L'une des vulnérabilités corrigées est exploitée sur l'Internet et a fait l'objet de l'alerte CERTA-2009-ALE-005.

### 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Les mises à jour pour Mac et Microsoft Works seront disponibles prochainement.

### 6 Documentation

- Bulletin de sécurité Microsoft MS08-017 du 12 mai 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-017.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS08-017.msp>
- Référence CVE CVE-2009-0220 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0220>
- Référence CVE CVE-2009-0221 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0221>
- Référence CVE CVE-2009-0222 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0222>
- Référence CVE CVE-2009-0224 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0224>
- Référence CVE CVE-2009-0225 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0225>
- Référence CVE CVE-2009-0226 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0226>
- Référence CVE CVE-2009-0227 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0227>
- Référence CVE CVE-2009-0556 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0556>
- Référence CVE CVE-2009-1128 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1128>
- Référence CVE CVE-2009-1129 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1129>
- Référence CVE CVE-2009-1130 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1130>
- Référence CVE CVE-2009-1131 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1131>
- Référence CVE CVE-2009-1137 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1137>

# **Gestion détaillée du document**

**13 mai 2009** version initiale.