

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : 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-2010-AVI-544>

---

### Gestion du document

Référence	CERTA-2010-AVI-544
Titre	Vulnérabilités dans Microsoft PowerPoint
Date de la première version	10 novembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-088 du 09 novembre 2010
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 2002 Service Pack 3 ;
- Microsoft PowerPoint 2003 Service Pack 3 ;
- Microsoft Office 2004 pour Mac ;
- Microsoft PowerPoint Viewer 2007 Service Pack2.

## 3 Résumé

Plusieurs vulnérabilités affectent Microsoft PowerPoint. Elles permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

## 4 Description

Deux vulnérabilités ont été corrigées dans Microsoft PowerPoint :

- un débordement de tampon lors du traitement d'un fichier PowerPoint 95 spécialement créé ;
- un débordement d'entier lors du traitement d'un fichier PowerPoint spécialement créé.

Ces vulnérabilités peuvent être exploitées par un attaquant distant pour exécuter du code arbitraire.

## 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 MS10-088 du 10 novembre 2010 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-088.aspx>  
<http://www.microsoft.com/technet/security/Bulletin/MS10-088.aspx>
- Référence CVE CVE-2010-2572 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2572>
- Référence CVE CVE-2010-2573 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2573>

## Gestion détaillée du document

10 novembre 2010 version initiale.