

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft Office, dont 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-2006-AVI-346>

Gestion du document

Référence	CERTA-2006-AVI-346
Titre	Multiples vulnérabilités dans Microsoft Office, dont Powerpoint
Date de la première version	09 août 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-048 du 08 août 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

- Microsoft Powerpoint 2000 dans Office 2000 Service Pack 3 ;
- Microsoft Powerpoint 2002 dans Office XP Service Pack 3 ;
- Microsoft Powerpoint 2003 dans Office 2003 (Service Pack 1 ou 2) ;
- Microsoft Powerpoint 2004 dans Office 2004 pour Mac ;
- Microsoft Powerpoint v.X dans Office v.X pour Mac.

La visionneuse Microsoft Powerpoint 2003 n'est pas affectée par ces vulnérabilités, ainsi que les produits de Microsoft Works Suite.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans Microsoft Office Powerpoint. Une personne malveillante peut construire des documents Powerpoint exploitant l'une d'elles afin d'exécuter des commandes arbitraires lorsqu'ils seront ouverts sur le système ayant une version vulnérable.

4 Description

Cet avis fait suite à la mise à jour de l'alerte CERTA-2006-ALE-009-002.

Plusieurs vulnérabilités ont été identifiées dans le logiciel de présentations Microsoft Office Powerpoint. L'une d'elles concerne la bibliothèque `mso.dll` utilisée par la suite Office.

Pour exploiter celles-ci, un utilisateur malveillant doit construire un document Powerpoint particulier, puis le distribuer (par courrier électronique, par lien dans une page Web, etc). Si un utilisateur l'ouvre sur un système vulnérable, il est alors possible d'exécuter des commandes arbitraires avec les droits de ce dernier.

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 MS06-048 du 08 août 2006 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS06-048.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS06-048.mspx>
- Référence CVE CVE-2006-3590 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3590>
- Référence CVE CVE-2006-3449 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3449>
- Référence à l'alerte CERTA CERTA-ALE-2006-009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-ALE-009/>

Gestion détaillée du document

09 août 2006 version initiale.