



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 octobre 2006
N° CERTA-2006-AVI-438

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-2006-AVI-438>

Gestion du document

Référence	CERTA-2006-AVI-438
Titre	Multiples vulnérabilités dans Microsoft PowerPoint
Date de la première version	11 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-058 du 10 octobre 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 ;
- exécution de code arbitraire ;
- contournement de la politique de sécurité.

2 Systèmes affectés

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

La visionneuse Microsoft Powerpoint 2003 (*Viewer*) ne serait pas affectée par ces vulnérabilités.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans l'application Microsoft Powerpoint, fournie dans la suite bureautique Microsoft Office pour manipuler des documents de présentations.

Une personne malveillante pourrait exploiter l'une d'elles en construisant un document Powerpoint particulier. Lorsque celui-ci est ouvert sur une machine ayant une version de Powerpoint vulnérable, il exécuterait du code arbitraire, et permettrait donc de prendre le contrôle de la machine.

4 Description

Plusieurs vulnérabilités ont été identifiées dans l'application Microsoft Powerpoint, fournie dans la suite bureautique Microsoft Office pour manipuler des documents de présentations. Parmi celles-ci :

- Powerpoint ne manipulerait pas correctement les documents Powerpoint contenant un pointeur d'objet incorrect.
- Powerpoint ne générerait pas de manière convenable les enregistrements de données de certains documents Powerpoint.
- un script Visual Basic (VB) utilisant la fonction `SlideShowWindows.View.GotoNamedShow()` et inséré dans un document de présentation perturberait Powerpoint.

Une personne malveillante pourrait exploiter l'une de ces vulnérabilités en construisant un document Powerpoint particulier. Lorsque celui-ci est ouvert sur une machine ayant une version de Powerpoint vulnérable, il exécuterait du code arbitraire, et permettrait donc de prendre le contrôle de la machine.

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 MS06-058 du 10 octobre 2006 :
<http://www.microsoft.com/france/technet/security/bulletin/MS06-058.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-058.msp>
- Référence CVE CVE-2006-3435 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3435>
- Référence CVE CVE-2006-3876 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3876>
- Référence CVE CVE-2006-3877 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3877>
- Référence CVE CVE-2006-4694 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4694>

Gestion détaillée du document

11 octobre 2006 version initiale.