



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 février 2010
N° CERTA-2010-AVI-062

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2010-AVI-062>

Gestion du document

Référence	CERTA-2010-AVI-062
Titre	Vulnérabilités de Microsoft PowerPoint
Date de la première version	10 février 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-004 du 09 février 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 Office PowerPoint 2002 Service Pack 3 (Office XP SP3) ;
- Microsoft Office PowerPoint 2003 Service Pack 3 ;
- Microsoft Office 2004 pour Mac.

3 Résumé

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

4 Description

Six vulnérabilités affectant Microsoft Powerpoint ont été publiées :

- un débordement de mémoire lors du traitement des chemins permet à un utilisateur malveillant distant de prendre le contrôle du système vulnérable ;

- un débordement du tas (*heap*) lors du traitement de certains fichiers permet à un utilisateur malveillant d'exécuter du code arbitraire à distance ;
- une erreur d'indexation dans un tableau est exploitable par un utilisateur malveillant pour exécuter du code arbitraire à distance ;
- une erreur d'allocation de la mémoire peut être mise à profit par un utilisateur malveillant pour exécuter du code arbitraire à distance ;
- deux débordements de piles d'objets lors du traitement de certains fichiers permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

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 MS10-004 du 09 février 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-004.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-004.msp>
- Référence CVE CVE-2010-0029 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0029>
- Référence CVE CVE-2010-0030 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0030>
- Référence CVE CVE-2010-0031 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0031>
- Référence CVE CVE-2010-0032 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0032>
- Référence CVE CVE-2010-0033 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0033>
- Référence CVE CVE-2010-0034 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0034>

Gestion détaillée du document

10 février 2010 version initiale.