

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité de 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-ALE-005>

Gestion du document

Référence	CERTA-2009-ALE-005-001
Titre	Vulnérabilité de PowerPoint
Date de la première version	03 avril 2009
Date de la dernière version	13 mai 2009
Source(s)	Bulletin de sécurité Microsoft 969136 du 02 avril 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 SP3, 2002 SP3 (XP SP3), 2003 SP3 ;
- Microsoft Office 2004 pour Mac.

3 Résumé

Une vulnérabilité de PowerPoint permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité de PowerPoint est exploitable par un utilisateur malveillant, par le biais d'un fichier PowerPoint spécialement conçu (.PPS ou .PPT). L'ouverture de ce fichier par un utilisateur du système vulnérable provoque l'exécution de code arbitraire avec les droits de cet utilisateur.

Cette vulnérabilité est actuellement exploitée. Des programmes malveillants (Exploit:Win32/Apptom pour Microsoft, Exploit:W32/Ppdropper pour F-secure...) circulent sur l'Internet.

5 Contournement provisoire

Dans l'attente d'un correctif, les mesures suivantes limitent la vulnérabilité du système :

- utiliser une version non vulnérable (voir section Documentation) ou un logiciel alternatif ;
- utiliser l'outil MOICE pour ouvrir un document suspect ;
- utiliser la fonctionnalité Microsoft Office File Block pour les documents des versions inférieures ou égales à 2003, soit par édition de la base de registre, soit par application d'une GPO. Les instructions détaillées sont données dans le bulletin Microsoft (voir section Documentation) ;
- ne pas ouvrir de document d'origine mal connue ou provenant de manière inattendue d'une source connue.

L'utilisation de l'ordinateur avec des droits limités permet d'atténuer l'impact de l'exploitation de la vulnérabilité.

6 Solution

Se référer à l'avis CERTA-2009-AVI-185 pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Avis CERTA-2009-AVI-185 du 13 mai 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-185/index.html>
- Bulletin de sécurité Microsoft 969136 du 02 avril 2009 :
<http://www.microsoft.com/technet/security/advisory/969136.msp>
- Référence CVE CVE-2009-0556 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0556>

Gestion détaillée du document

03 avril 2009 version initiale.

13 mai 2009 mise à disposition d'un correctif par l'éditeur, ajout de la référence de l'avis correspondant.