

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-2011-AVI-282>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2011-AVI-282 |
| Titre | Vulnérabilités dans Microsoft PowerPoint |
| Date de la première version | 11 mai 2011 |
| Date de la dernière version | – |
| Source | Bulletin de sécurité Microsoft MS11-036 du 10 mai 2011 |
| 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 :

- XP SP3 ;
- 2003 SP3 ;
- 2004 pour Mac ;
- 2007 SP2 ;
- 2008 pour Mac ;
- Pack de compatibilité pour les formats de fichiers 2007 SP2 ;
- Convertisseur Open XML pour Mac.

3 Résumé

Deux vulnérabilités dans Powerpoint permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Deux vulnérabilités de Powerpoint ont été corrigées :

- une présentation PowerPoint spécialement formée permet de provoquer une corruption de la mémoire. Celle-ci peut être exploitée par un utilisateur malveillant pour exécuter du code avec les droits de l'utilisateur qui ouvre cette présentation ;
- une présentation PowerPoint spécialement formée permet de provoquer un débordement de zone mémoire. Celui-ci peut être exploité par un utilisateur malveillant pour exécuter du code avec les droits de l'utilisateur qui ouvre cette présentation.

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 MS11-036 du 10 mai 2011 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-036.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS11-036.msp>
- Référence CVE CVE-2011-1269 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1269>
- Référence CVE CVE-2011-1270 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1270>

Gestion détaillée du document

11 mai 2011 version initiale.