



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 octobre 2008
N° CERTA-2006-ALE-012-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité 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-2006-ALE-012>

Gestion du document

| | |
|-----------------------------|--|
| Référence | CERTA-2006-ALE-012-001 |
| Titre | Vulnérabilité de Microsoft PowerPoint |
| Date de la première version | 13 octobre 2006 |
| Date de la dernière version | 09 octobre 2008 |
| Source(s) | Note du MSRC (Microsoft Security Response Center) du 12 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 ;
- déni de service.

2 Systèmes affectés

- Microsoft PowerPoint 2003 ;
- Microsoft PowerPoint XP.

3 Résumé

Une vulnérabilité a été découverte sur le logiciel Microsoft PowerPoint.

4 Description

Une vulnérabilité a été découverte sur le logiciel Microsoft PowerPoint versions 2003 et XP. Aucune mise à jour n'est disponible pour celle-ci.

Un code d'exploitation provoquant un déni de service (arrêt inopiné) du logiciel est disponible sur l'Internet. Ce code d'exploitation a été validée sur PowerPoint XP. L'impact réel (autre le déni de service) de cette vulnérabilité n'est pas encore connu.

Aucune précision n'est disponible pour le moment quant à l'extension de cette vulnérabilité aux autres versions de Microsoft PowerPoint.

5 Contournement provisoire

N'ouvrir que les documents bureautiques de confiance, et utiliser une suite bureautique alternative à jour (OpenOffice, par exemple).

6 Solution

Microsoft a corrigé cette vulnérabilité dans le service pack 3 de Office 2003. La vulnérabilité n'est toujours pas corrigée pour PowerPoint XP. Toutefois, l'éditeur affirme que cette faille ne permet pas d'exécuter du code arbitraire. Cette vulnérabilité ne justifiant donc plus le même niveau de vigilance, le CERTA a décidé de réévaluer l'alerte.

7 Documentation

- Bloc-notes du MSRC (Microsoft Security Response Center) :
<http://blogs.technet.com/msrc/archive/2006/10/12/poc-published-for-ms-office-2003-powerpoint.aspx>

Gestion détaillée du document

13 octobre 2006 version initiale.

09 octobre 2008 ajout du correctif pour PowerPoint 2003 et réévaluation de l'alerte.