

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité de la librairie MSO.DLL dans Microsoft Office

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-009>

Gestion du document

Référence	CERTA-2006-ALE-009-002
Titre	Vulnérabilité de la librairie MSO.DLL dans Microsoft Office
Date de la première version	15 juillet 2006
Date de la dernière version	09 août 2006
Source(s)	
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 ;
- déni de service à distance.

2 Systèmes affectés

- Microsoft Powerpoint dans Microsoft Office XP ;
- Microsoft Powerpoint 2002 dans Microsoft Office 2003 ;
- Microsoft Powerpoint 2003 dans Office 2000 ;
- Microsoft Powerpoint dans Office 2004 pour MacOS.

Microsoft Office concerne une suite d'applications, incluant Excel, FrontPage, Outlook, Powerpoint, Publisher et Word.

La visionneuse de documents Powerpoint (Microsoft Powerpoint Viewer) ne serait pas affectée par cette vulnérabilité.

3 Résumé

Une vulnérabilité non corrigée dans une librairie de Microsoft Office permettrait à un utilisateur mal intentionné d'exécuter du code arbitraire ou de provoquer un déni de service à distance. Un code en circulation exploite cette vulnérabilité par le biais de documents Powerpoint.

4 Description

Les fonctions `mso` (Microsoft Office) sont des fonctions spéciales disponibles dans la librairie `mso.dll` d'Office. Elles s'occupent par exemple des affichages de bulles, des barres de menu, des boîtes de dialogue, etc. Ces fonctions sont appelées par plusieurs applications de Microsoft Office, notamment Word ou Powerpoint.

Une vulnérabilité a été identifiée dans la librairie `mso.dll`. Elle fait l'objet d'une utilisation par du code malveillant sur l'Internet. Elle est exploitée par le biais d'un document `Powerpoint`.

Powerpoint serait également impacté par deux autres vulnérabilités. Cette information n'est pas confirmée pour le moment.

5 Contournement provisoire

5.1 Utiliser les visionneuses Office dans la mesure du possible

La visionneuse de documents Powerpoint ne serait pas affectée par les vulnérabilités précédentes.

5.2 Mettre à jour la base de signatures d'antivirus

Certains éditeurs d'antivirus proposent déjà des mises à jour de signatures prenant en compte le code malveillant sous sa forme actuelle. Il est cependant probable que des variantes apparaissent afin de contourner ces signatures.

5.3 Filter les pièces jointes au niveau de la passerelle de la messagerie

Les passerelles de messagerie offrent le plus souvent la possibilité de filtrer les documents en pièce jointe. Dans les cas les plus simples, elles se basent sur l'extension du nom du fichier. Dans la mesure du possible, il est conseillé de filtrer les extensions `.ppt` venant de domaines externes.

5.4 Ouvrir les documents provenant de sources de confiance

A la réception d'un document Office (au format `.ppt` compte tenu du code malveillant actuel), soit par le biais de la messagerie électronique ou sur tout autre support, il est nécessaire de s'assurer de la provenance de ce fichier et de ne l'ouvrir que si la source est de confiance.

6 Solution

Appliquer le correctif MS06-048 de l'éditeur Microsoft (Cf. section documentation).

7 Documentation

- Bulletin de sécurité Microsoft MS06-048 du 08 août 2006 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS06-046.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-048.msp>
- Référence CVE CVE-2006-3493 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3493>
- Référence CVE CVE-2006-3656 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3656>
- Référence CVE CVE-2006-3655 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3655>

- Référence CVE CVE-2006-3660 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3660>
- Référence CVE CVE-2006-3590 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3590>
- Téléchargement de la visionneuse Microsoft Powerpoint :
<http://www.microsoft.com/downloads/Products.aspx?displaylang=fr>
- Memento du CERTA sur les virus informatiques :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-MEM-001.pdf>
- Avis CERTA CERTA-2006-AVI-346 du 09 août 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-346/>

Gestion détaillée du document

15 juillet 2006 version initiale.

18 juillet 2006 ajout de références.

09 août 2006 ajout du correctif MS06-048 de Microsoft et de l'avis CERTA-2006-AVI-346.