

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft Word

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-AVI-440>

Gestion du document

Référence	CERTA-2006-AVI-440
Titre	Multiples vulnérabilités dans Microsoft Word
Date de la première version	11 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-060 du 10 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 à distance ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

- Microsoft Word 2000 dans la suite bureautique Microsoft Office 2000 Service Pack 3 ;
- Microsoft Word 2002 dans la suite bureautique Microsoft Office XP Service Pack 3 ;
- Microsoft Word 2003 dans la suite bureautique Microsoft Office 2003 Service Pack 1 ou 2 ;
- Microsoft Word 2004 dans la suite bureautique Microsoft Office 2004 pour Mac ;
- Microsoft Word v.X dans la suite bureautique Microsoft Office v.X pour Mac ;
- Suite Microsoft Works 2004 ;
- Suite Microsoft Works 2005 ;
- Suite Microsoft Works 2006 ;
- Visionneuse Microsoft Office Word 2003 (*Viewer*).

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans l'application Microsoft Word, fournie dans la suite bureautique Microsoft Office ou dans Microsoft Works.

Une personne malveillante pourrait exploiter l'une d'elles en construisant un document Word particulier. Lorsque celui-ci est ouvert sur une machine ayant une version de Word vulnérable, il exécuterait du code arbitraire, et permettrait donc de prendre le contrôle de la machine.

4 Description

Plusieurs vulnérabilités ont été identifiées dans l'application Microsoft Word, fournie dans la suite bureautique Microsoft Office ou dans Microsoft Works. Parmi celles-ci :

- Microsoft Word ne manipulerait pas convenablement certaines chaînes de caractères incluses dans les documents.
- Microsoft Word ne traiterai pas de manière correcte certains documents de type *publipostage* (ou *mail merge*). Ce type permet notamment d'imprimer des documents contenant différentes coordonnées de personnes sous un format donné.

Une personne malveillante pourrait exploiter l'une de ces vulnérabilités en construisant un document Word particulier. Lorsque celui-ci est ouvert sur une machine ayant une version de Word vulnérable, il exécuterait du code arbitraire, et permettrait donc de prendre le contrôle de la machine.

5 Solution

Se référer au bulletin de sécurité MS06-060 de l'éditeur Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS06-060 du 10 octobre 2006 :
<http://www.microsoft.com/france/technet/security/bulletin/MS06-060.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-060.msp>
- Référence CVE CVE-2006-3647 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3647>
- Référence CVE CVE-2006-3651 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3651>
- Référence CVE CVE-2006-4534 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4534>
- Référence CVE CVE-2006-4693 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4693>

Gestion détaillée du document

11 octobre 2006 version initiale.