

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft Excel

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-439>

Gestion du document

Référence	CERTA-2006-AVI-439-001
Titre	Multiples vulnérabilités dans Microsoft Excel
Date de la première version	11 octobre 2006
Date de la dernière version	15 décembre 2006
Source(s)	Bulletin de sécurité Microsoft MS06-059 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 Excel 2000 dans la suite bureautique Microsoft Office 2000 Service Pack 3 ;
- Microsoft Excel 2002 dans la suite bureautique Microsoft Office XP Service Pack 3 ;
- Microsoft Excel 2003 dans la suite bureautique Microsoft Office 2003 Service Pack 1 ou 2 ;
- Microsoft Excel 2004 dans la suite bureautique Microsoft Office 2004 pour Mac ;
- Microsoft Excel 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 Excel 2003 (*Viewer*).

3 Résumé

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

Une personne malveillante pourrait exploiter l'une d'elles en construisant un document Excel particulier. Lorsque celui-ci est ouvert sur une machine ayant une version d'Excel 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 Excel, fournie dans la suite bureautique Microsoft Office ou dans Microsoft Works. Parmi celles-ci :

- Excel ne manipulerait pas convenablement des documents `.xls` contenant un champ d'enregistrement `DATETIME` incorrect ;
- Excel ne manipulerait pas convenablement des documents `.xls` contenant un champ d'enregistrement `STYLE` incorrect. Le code d'exploitation en circulation utilise une chaîne de caractères particulière codés sur 2 octets (caractères asiatiques), qu'il est possible de désactiver en changeant la valeur `InstallLanguage` dans la table de registres ;
- Excel ne manipulerait pas convenablement des documents `.xls` contenant un champ d'enregistrement `COLINFO` incorrect ;
- Des fichiers Lotus 1-2-3 ne seraient pas traités de manière correct par Excel.

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

5 Solution

L'éditeur Microsoft vient de publier un nouveau correctif de sécurité destiné à mettre à jour l'exécutable `excel.exe`.

Se référer au bulletin de sécurité MS06-059 de l'éditeur Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS06-059 du 10 octobre 2006 :
<http://www.microsoft.com/france/technet/security/bulletin/MS06-059.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS06-059.msp>
- Mise à jour du bulletin de sécurité Microsoft MS06-059 du 12 décembre 2006 :
<http://support.microsoft.com/kb/924164>
- Référence CVE CVE-2006-2387 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2387>
- Référence CVE CVE-2006-3431 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3431>
- Référence CVE CVE-2006-3867 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3867>
- Référence CVE CVE-2006-3875 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3875>

Gestion détaillée du document

11 octobre 2006 version initiale.

15 décembre 2006 ajout de la référence de la mise à jour du bulletin de sécurité Microsoft MS06-059.