

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs 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-2007-AVI-203>

Gestion du document

Référence	CERTA-2007-AVI-203
Titre	Plusieurs vulnérabilités dans Microsoft Excel
Date de la première version	09 mai 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-203 du 08 mai 2007
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 Excel 2000 dans la suite Office 2000 Service Pack 3 ;
- Microsoft Excel 2002 dans la suite Office XP Service Pack 3 ;
- Microsoft Excel 2003 dans la suite Office 2003 Service Pack 2 ;
- Microsoft Excel 2003 Viewer dans la suite Office 2003 Service Pack 2 ;
- Microsoft Excel 2007 dans la suite Office 2007 ;
- Pack de compatibilité des formats de fichiers pour Excel 2007 ;
- Microsoft Office 2004 pour Mac.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans l'outil de bureautique Excel, inclus dans la suite Microsoft Office. L'exploitation de ces dernières peut conduire à l'exécution de code arbitraire sur la machine contenant une version vulnérable de l'application.

4 Description

Trois vulnérabilités ont été identifiées dans l'outil de bureautique Excel, inclus dans la suite Microsoft Office :

1. l'application ne manipulerait pas correctement des fichiers Excel contenant des enregistrements de type BIFF (pour *Binary Interchange File Format*). Il s'agit du format d'enregistrement commun d'Excel, qui se décline suivant plusieurs versions (BIFF8 pour Excel 2000, ou BIFF8X pour Excel 2002 et Excel 2003). L'exploitation de cette vulnérabilité provoque un débordement de mémoire, permettant une exécution de code arbitraire.
2. l'application ne manipulerait pas correctement des fichiers Excel contenant des valeurs particulières qui devraient indiquer une police de caractères. L'exploitation de cette vulnérabilité provoque également un débordement de mémoire, permettant une exécution de code arbitraire.
3. l'application ne manipulerait pas correctement des fichiers Excel contenant des enregistrements de filtres particuliers. L'exploitation de cette vulnérabilité provoque aussi un débordement de mémoire.

5 Solution

Se référer au bulletin de sécurité MS07-023 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS07-023 du 08 mai 2007 :
<http://www.microsoft.com/france/technet/security/bulletin/MS07-023.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-023.msp>
- Référence CVE CVE-2007-0215 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0215>
- Référence CVE CVE-2007-1203 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1203>
- Référence CVE CVE-2007-1214 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1214>

Gestion détaillée du document

09 mai 2007 version initiale.