



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 janvier 2007
N° CERTA-2007-AVI-016

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de 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-016>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2007-AVI-016 |
| Titre | Multiples vulnérabilités de Microsoft Excel |
| Date de la première version | 10 janvier 2007 |
| Date de la dernière version | – |
| Source(s) | Bulletin Microsoft MS07-002 |
| 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, 2002, 2003 ;
- Microsoft Excel Viewer 2003 ;
- Microsoft Works Suite 2004 et 2005 ;
- Microsoft Office 2004 et v. X pour Mac.

3 Résumé

Plusieurs vulnérabilités d'Excel permettent à un utilisateur malveillant d'exécuter un code arbitraire à distance.

4 Description

Plusieurs vulnérabilités affectent *Excel* :

- le traitement défectueux des fichiers contenant un enregistrement *IMDATA* mal formé permet à un utilisateur malveillant d'exécuter un code arbitraire sur le système vulnérable avec les droits de l'utilisateur ;
- le traitement défectueux des fichiers contenant un enregistrement *COLUMN* mal formé permet à un utilisateur malveillant d'exécuter un code arbitraire sur le système vulnérable avec les droits de l'utilisateur ;
- le traitement défectueux des fichiers contenant un enregistrement *PALETTE* mal formé permet à un utilisateur malveillant d'exécuter un code arbitraire sur le système vulnérable avec les droits de l'utilisateur ;
- le traitement défectueux des fichiers contenant une chaîne de caractères mal formée permet à un utilisateur malveillant d'exécuter un code arbitraire sur le système vulnérable avec les droits de l'utilisateur ;
- le traitement défectueux des fichiers contenant un enregistrement mal formé permet à un utilisateur malveillant d'exécuter un code arbitraire sur le système vulnérable avec les droits de l'utilisateur ;

Un attaquant peut exploiter ces vulnérabilités à distance en expédiant un courriel contenant un fichier spécialement conçu ou en incitant l'utilisateur à télécharger un tel fichier sur un site web.

Si l'utilisateur qui exécute le logiciel vulnérable est connecté sous une session d'administrateur, l'attaquant peut prendre le contrôle total de la machine.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS07-002 du 09 janvier 2007 :
<http://www.microsoft.com/france/technet/security/bulletin/MS07-002.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-002.msp>
- référence CVE CVE-2007-0027 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0027>
- référence CVE CVE-2007-0028 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0028>
- référence CVE CVE-2007-0029 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0029>
- référence CVE CVE-2007-0030 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0030>
- référence CVE CVE-2007-0031 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0031>

Gestion détaillée du document

10 janvier 2007 version initiale.