



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 novembre 2003
N° CERTA-2003-AVI-186

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft Word et 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-2003-AVI-186>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2003-AVI-186 |
| Titre | Vulnérabilités dans Microsoft Word et Microsoft Excel |
| Date de la première version | 12 novembre 2003 |
| Date de la dernière version | – |
| Source(s) | Bulletin de Microsoft MS03-050 |
| 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.

2 Systèmes affectés

- Microsoft Excel 97 ;
- Microsoft Excel 2000 ;
- Microsoft Excel 2002 ;
- Microsoft Word 97 ;
- Microsoft Word 98(J) ;
- Microsoft Word 2000 ;
- Microsoft Word 2002 ;
- Microsoft Works Suite 2001 ;
- Microsoft Works Suite 2002 ;
- Microsoft Works Suite 2003 ;
- Microsoft Works Suite 2004.

Microsoft Office Word 2003 et Microsoft Office Excel 2003 ne sont pas affectés.

3 Résumé

Deux vulnérabilités, l'une concernant Microsoft Excel, l'autre Microsoft Word, permettent l'exécution de code arbitraire.

4 Description

Une première vulnérabilité affecte Microsoft Excel. Celle-ci permet l'exécution automatique d'une macro judicieusement composée au moment de l'ouverture d'une feuille de calcul Excel, quelque soit le modèle de sécurité des macros.

Une seconde vulnérabilité concerne la vérification de la longueur de la valeur des données (noms des macros) contenue dans un document. Un utilisateur mal intentionné peut, au moyen d'un document Word judicieusement composé, exécuter du code arbitraire.

5 Solution

Appliquer les correctifs de l'éditeur :

<http://www.microsoft.com/technet/security/bulletin/ms03-050.asp>

6 Documentation

Bulletin de Microsoft MS03-050 :

<http://www.microsoft.com/technet/security/bulletin/ms03-050.asp>

Référence CVE CAN-2003-0820 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0820>

Référence CVE CAN-2003-0821 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0821>

Gestion détaillée du document

12 novembre 2003 version initiale.