



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 juillet 2006
N° CERTA-2006-ALE-007-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité 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-ALE-007>

Gestion du document

Référence	CERTA-2006-ALE-007-002
Titre	Vulnérabilité dans Microsoft Excel
Date de la première version	16 juin 2006
Date de la dernière version	12 juillet 2006
Source(s)	Article sur le site du Microsoft Security Response Center
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 ;
- déni de service.

2 Systèmes affectés

- Microsoft Excel 2000 Service Pack 3 ;
- Microsoft Excel 2002 Service Pack 3 ;
- Microsoft Excel 2003 Service Pack 1 ;
- Microsoft Excel 2003 Service Pack 2 ;
- Microsoft Excel Viewer 2003 ;
- Microsoft Office 2000 ;
- Microsoft Office 2003 ;
- Microsoft Office XP ;
- Microsoft Excel 2004 pour Mac ;
- Microsoft Excel version X pour Mac.

3 Résumé

Une vulnérabilité non corrigée dans Microsoft Excel permettrait à un utilisateur mal intentionné de faire exécuter du code arbitraire ou de provoquer un déni de service sur la machine d'un utilisateur ouvrant un fichier au format `xls`.

4 Description

Une vulnérabilité de nature pour le moment inconnue dans Microsoft Excel permettrait à un utilisateur mal intentionné d'exécuter du code arbitraire ou de provoquer un déni de service. Cette vulnérabilité ferait l'objet d'une utilisation par du code malveillant véhiculé via du pourriel (« spam ») sur l'Internet. Elle est exploitable par le biais d'un fichier `xls` construit de façon particulière. Cependant, l'attaque ne peut aboutir que si l'utilisateur décide d'ouvrir le fichier Excel.

5 Contournements provisoires

5.1 N'ouvrir que les documents provenant de sources de confiance

A la réception d'un document au format `xls` via la messagerie électronique ou par tout autre support (URL, clef USB, disquette, etc. . .), il est nécessaire de s'assurer de la provenance de ce fichier et de ne l'ouvrir que si la source est de confiance.

5.2 Utiliser un logiciel alternatif

Il est possible d'utiliser un tableur alternatif non affecté par la vulnérabilité comme `Gnumeric` ou celui de `OpenOffice.org`.

5.3 Contournement spécifique à Excel 2003

Microsoft Excel doit passer en mode «Repair» pour mettre en œuvre la vulnérabilité. Aussi, dans l'attente d'un correctif, il est recommandé de désactiver cette fonctionnalité de mode « Repair » en modifiant des clefs de la base de registres. Il est cependant important de noter qu'une erreur de modification dans la base de registres peut entraîner des dysfonctionnements voir la nécessité de réinstaller la machine.

sous windows 2000 :

- cliquer sur Démarrer puis Exécuter. taper `regedt32` et cliquer sur ok ;
- éditer la clef `HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency` (si cette clef n'existe pas, la créer) ;
- cliquer sur Editer puis permissions ;
- cliquer afin de décocher la case `Allow Inheritable Permissions from the parent to propagate to this object.` cliquer alors sur Supprimer puis OK ;
- un message d'avertissement apparaît alors, cliquer sur Oui.

sous windows XP Service Pack 1 et suivant :

- cliquer sur Démarrer puis Exécuter. taper `regedt32` et cliquer sur ok ;
- éditer la clef `HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Excel\Resiliency` (si cette clef n'existe pas, la créer) ;
- cliquer sur Editer puis permissions ;
- cliquer afin de décocher la case `Inherit from the parent the permission entries that apply to child objects. Include these with entries explicitly defined here.` cliquer alors sur Supprimer puis OK ;
- un message d'avertissement apparaît alors, cliquer sur Oui.

NB: Le mode « Repair » de Microsoft Excel a pour fonction de récupérer les documents Excel endommagés. En appliquant ce contournement provisoire, il sera impossible d'utiliser cette fonctionnalité de récupération.

6 Solution

Se référer au bulletin de sécurité de l'éditeur et à l'avis de sécurité du CERTA pour l'obtention du correctif.

7 Documentation

- Bulletin de sécurité Microsoft MS06-037 du 11 juillet 2006 :
<http://www.microsoft.com/technet/security/Bulletin/MS06-037.msp>
<http://www.microsoft.com/france/technet/security/Bulletin/MS06-037.msp>
- Avis de sécurité du CERTA du 12 juillet 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-285/index.html>
- Site du Microsoft Security Response Center :
<http://blogs.technet.com/msrc/archive/2006/06/16/436174.aspx>
- Bulletin du SANS du 16 juin 2006 :
<http://isc.sans.org/diary.php/storyid=1420>
- Référence CVE CVE-2006-3059 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3059>

Gestion détaillée du document

16 juin 2006 version initiale ;

20 juin 2006 ajout du contournement provisoire pour Windows 2003, ajout des versions Mac et du Viewer, ajout de la référence CVE.

12 juillet 2006 ajout des références aux bulletins de sécurité Microsoft et CERTA.