

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Microsoft Office

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-ALE-004>

Gestion du document

Référence	CERTA-2007-ALE-004-005
Titre	Vulnérabilité dans Microsoft Office
Date de la première version	03 février 2007
Date de la dernière version	13 février 2007
Source(s)	Avis de sécurité Microsoft 932553 du 02 février 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.
- Déni de service à distance.

2 Systèmes affectés

- Microsoft Office 2000 ;
- Microsoft Office XP ;
- Microsoft Office 2003 ;
- Microsoft Office 2004 pour Mac.

3 Résumé

Une vulnérabilité a été identifiée dans Microsoft Office. Elle est actuellement exploitée par le biais de l'application Excel. Une personne malveillante pourrait diffuser un fichier spécialement construit (en pièce jointe d'un courrier électronique, ou par téléchargement sur une page Web par exemple), afin de provoquer, lors de son ouverture, l'exécution de code arbitraire sur la machine vulnérable.

4 Description

Une vulnérabilité a été identifiée dans Microsoft Office. Il s'agirait d'une mauvaise interprétation d'une chaîne de caractères dans un fichier Office qui provoquerait un débordement de mémoire. Une personne malveillante pourrait diffuser un fichier spécialement construit (en pièce jointe d'un courrier électronique, ou par téléchargement sur une page Web par exemple), afin de provoquer, lors de son ouverture, l'exécution de code arbitraire sur la machine vulnérable.

Un code exploitant cette vulnérabilité est actuellement en circulation. Il se présente sous la forme d'un fichier Excel, et permettrait d'installer un Cheval de Troie sous Windows XP Service Pack 2. Il provoquerait sinon une perturbation (*fermeture inopinée*) de l'application Excel sur d'autres versions du système d'exploitation Microsoft Windows.

L'éditeur d'anti-virus McAfee le prénomme `Exploit-MSExcel.h`. Il se caractérise par la création d'un fichier `top10.exe` dans le répertoire `TEMP`.

Il n'existe pas de correctif officiel pour le moment.

5 Contournement provisoire

5.1 Utiliser un logiciel alternatif

Le CERTA recommande d'utiliser des applications alternatives pour visualiser les documents Office, et notamment, pour les fichiers au format Excel, des tableurs comme `Gnumeric` ou celui de `OpenOffice.org`.

5.2 Mettre à jour la base de signatures d'antivirus

Certains éditeurs d'antivirus proposent déjà des mises à jours de signatures prenant en compte les codes malveillants sous sa forme actuelle. Il est cependant probable que des variantes apparaissent afin de contourner ces antivirus.

5.3 Filtrer les pièces jointes au niveau des passerelles

Dans la mesure du possible, il est recommandé de filtrer les fichiers au format Excel (extension `.xls`) au niveau des passerelles (messagerie, web ...).

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

A la réception d'un document au format Excel soit par le biais de la messagerie électronique ou sur tout autre support, il est nécessaire de s'assurer de la provenance de ce fichier et de ne l'ouvrir que si la source est de confiance et après analyse par un antivirus à jour.

5.5 Limiter l'impact en utilisant un compte utilisateur sans privilège

L'utilisation de compte n'ayant pas de droits d'administration permet de limiter l'infection au contexte de l'utilisateur.

6 Solution

Appliquer les correctifs tel que décrit sur le site de l'éditeur (cf. Documentation);

7 Documentation

- Bulletins de mise à jour Microsoft MS07-014 et MS07-015 du 13 février 2007 :
<http://www.microsoft.com/technet/security/bulletin/ms07-014.msp>
<http://www.microsoft.com/technet/security/bulletin/ms07-015.msp>
- Avis du CERTA numero CERTA-2007-AVI-083 du 14 février 2007:
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-083/index.html>

- Avis de sécurité Microsoft 932553 du 02 février 2007 :
<http://www.microsoft.com/technet/security/advisory/932553.msp>
- Référence CVE CVE-2007-0671 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0671>
- Annonce du laboratoire de McAfee du 02 février 2007 :
<http://www.avertlabs.com/research/blog/?p=191>

Gestion détaillée du document

03 février 2007 version initiale.

13 février 2007 Ajout de la solution.