

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-2009-ALE-002>

Gestion du document

Référence	CERTA-2009-ALE-002-001
Titre	Vulnérabilité dans Microsoft Excel
Date de la première version	25 février 2009
Date de la dernière version	15 avril 2009
Source(s)	Avis de sécurité Microsoft 968272 du 24 février 2009 Bulletin de sécurité Microsoft MS09-009 du 14 avril 2009
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 Office Excel 2000 Service Pack 3 ;
- Microsoft Office Excel 2002 Service Pack 3 ;
- Microsoft Office Excel 2003 Service Pack 3 ;
- Microsoft Office Excel 2007 Service Pack 1 ;
- Microsoft Office Excel Viewer 2003 ;
- Microsoft Office Excel Viewer 2003 Service Pack 3 ;
- Microsoft Office Excel Viewer ;
- Microsoft Office Compatibility Pack pour Word, Excel et Powerpoint 2007, Service Pack 1 ;
- Microsoft Office 2004 pour Mac ;
- Microsoft Office 2008 pour Mac.

3 Résumé

Une vulnérabilité a été identifiée sur Microsoft Excel. L'exploitation de cette dernière par le biais d'un document spécialement conçu permet à une personne malveillante d'exécuter du code arbitraire à distance sur un poste ayant une version vulnérable de l'application.

4 Description

Une vulnérabilité a été identifiée sur l'application bureautique Microsoft Excel.

L'exploitation de cette vulnérabilité par le biais d'un document XLS spécialement conçu permet à une personne malveillante d'exécuter du code arbitraire à distance sur un poste ayant une version vulnérable de l'application.

5 Contournement provisoire

Dans l'attente d'un correctif, plusieurs mesures permettent de réduire l'impact de l'exploitation de cette vulnérabilité :

- travailler avec un compte utilisateur aux droits restreints (principe du moindre privilège) ;
- utiliser l'outil de conversion MOICE (Microsoft Office Isolated Conversion Environment) pour convertir tout fichier XLS en XSLX avant son ouverture ;
- activer la mesure (très restrictive) FileBlock, imposant l'ouverture unique des fichiers au nouveau format XML. Les détails pratiques se trouvent dans l'avis de sécurité Microsoft ;
- utiliser un logiciel alternatif (visualisateur, tableur ou suite bureautique) ;
- n'ouvrir que des documents issus de sources de confiance ;
- être circonspect à l'égard des pièces jointes de courriels et des documents téléchargés.

6 Solution

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

7 Documentation

- Bulletin de sécurité Microsoft MS09-009 du 14 avril 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-009.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-009.msp>
- Avis de sécurité Microsoft 968272 du 24 février 2009 :
<http://www.microsoft.com/technet/security/advisory/968272.msp>
- Article du bloc-notes MSRC correspondant :
<http://blogs.technet.com/msrc/archive/2009/02/24/microsoft-security-advisory-968272.aspx>
- Article du bloc-notes SWI correspondant :
<http://blogs.technet.com/swi/archive/2009/02/24/more-information-about-the-new-excel-vulnerability.aspx>
- Référence CVE CVE-2009-0100 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0100>
- Référence CVE CVE-2009-0238 :
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0238>
- Avis du CERTA numéro CERTA-2009-AVI-147 du 15 avril 2009 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-ALE-002/index.html>

Gestion détaillée du document

25 février 2009 version initiale.

15 avril 2009 ajout du lien vers le correctif.