

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités 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-2008-AVI-404>

Gestion du document

Référence	CERTA-2008-AVI-404
Titre	Vulnérabilités dans Microsoft Excel
Date de la première version	13 août 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-043 du 12 août 2008
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 Service Pack 3 ;
- Microsoft Excel 2002 Service Pack 3 ;
- Microsoft Excel 2003 Service Pack 2 ;
- Microsoft Excel 2003 Service Pack 3 ;
- Microsoft Excel 2007 ;
- Microsoft Excel 2007 Service Pack 1 ;
- Microsoft Office Excel Viewer 2003 ;
- Microsoft Office Excel Viewer 2003 Service Pack ;
- Microsoft Office Excel Viewer ;
- Microsoft Office Compatibility Pack pour les formats Office 2007 ;
- Microsoft Office Compatibility Pack pour les formats Office 2007 Service Pack 1 ;
- Microsoft Office SharePoint Server 2007 ;
- Microsoft Office SharePoint Server 2007 Service Pack 1 ;

- Microsoft Office SharePoint Server 2007 x64 Edition ;
- Microsoft Office SharePoint Server 2007 Service Pack 1 x64 Edition ;
- Microsoft Office 2004 pour Mac ;
- Microsoft Office 2008 pour Mac.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans l'application bureautique Microsoft Excel. Elles peuvent être exploitées à distance via un fichier spécialement construit afin d'exécuter des commandes arbitraires sur le système vulnérable sur lequel le document serait ouvert.

4 Description

Plusieurs vulnérabilités ont été identifiées dans l'application bureautique Microsoft Excel :

- l'application ne manipule pas correctement les enregistrements `FORMAT` dans un document Excel servant à l'indexation de tables ;
- l'application ne manipule pas correctement les enregistrements `AxesSet` de graphiques inclus dans un document Excel ;
- l'application ne traite pas correctement les formats de fichiers `BIFF` et en particulier les enregistrements `COUNTRY` ;
- l'application ne détruit pas correctement la chaîne de caractères servant de mot de passe quand le fichier est paramétré pour ne pas paramétrer le mot de passe de session de données distant.

Ces vulnérabilités peuvent être exploitées et provoquer une corruption de mémoire afin d'exécuter du code arbitraire.

5 Solution

Se référer au bulletin de sécurité MS08-043 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-043 du 12 août 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-043.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS08-043.mspx>
- Référence CVE CVE-2008-3003 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3003>
- Référence CVE CVE-2008-3004 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3004>
- Référence CVE CVE-2008-3005 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3005>
- Référence CVE CVE-2008-3006 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3006>
- Avis de sécurité iDefense du 12 août 2008 :
<http://labs.idefense.com/intelligence/vulnerabilities/>
- Avis de sécurité TippingPoint ZDI-08-048 du 12 août 2008 :
<http://www.zerodayinitiative.com/advisories/ZDI-08-048>

Gestion détaillée du document

13 août 2008 version initiale.