

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft Office 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-2010-AVI-250>

Gestion du document

Référence	CERTA-2010-AVI-250
Titre	Multiples vulnérabilités dans Microsoft Office Excel
Date de la première version	09 juin 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-038 du 08 juin 2010
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 2002 SP3 ;
- Microsoft Office Excel 2003 SP3 ;
- Microsoft Office Excel 2007 SP1 et SP2 ;
- Microsoft Office 2004 pour Mac ;
- Microsoft Office 2008 pour Mac ;
- Open XML File Format Converter pour Mac ;
- Microsoft Office Excel Viewer SP1 et SP2 ;
- Microsoft office Compatilby Pack pour Word, Excel et Power Point 2007 File Formats SP1 et SP2.

3 Résumé

Quatorze vulnérabilités signalées confidentiellement dans Microsoft Office ont été corrigées. Elles permettent, entre autre, l'exécution de code arbitraire à distance.

4 Description

Quatorze vulnérabilités signalées confidentiellement dans Microsoft Office ont été corrigées. Certaines sont exploitables au moyen d'un fichier Excel spécifiquement réalisé permettant ainsi à une personne malintentionnée d'exécuter du code arbitraire à distance, et cela avec les droits de l'utilisateur victime. Ce bulletin de sécurité remplace le MS10-017 pour les systèmes affectés listés ci-dessus.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS10-038 du 08 juin 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-038.aspx>
<http://www.microsoft.com/technet/security/Bulletin/MS10-038.aspx>
- Référence CVE CVE-2010-0821 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0821>
- Référence CVE CVE-2010-0822 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0822>
- Référence CVE CVE-2010-0823 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0823>
- Référence CVE CVE-2010-0824 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0824>
- Référence CVE CVE-2010-1245 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1245>
- Référence CVE CVE-2010-1246 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1246>
- Référence CVE CVE-2010-1247 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1247>
- Référence CVE CVE-2010-1248 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1248>
- Référence CVE CVE-2010-1249 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1249>
- Référence CVE CVE-2010-1250 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1250>
- Référence CVE CVE-2010-1251 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1251>
- Référence CVE CVE-2010-1252 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1252>
- Référence CVE CVE-2010-1253 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1253>
- Référence CVE CVE-2010-1254 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1254>

Gestion détaillée du document

09 juin 2010 version initiale.