

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples 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-2011-AVI-204>

---

### Gestion du document

Référence	CERTA-2011-AVI-204
Titre	Multiples vulnérabilités dans Microsoft Excel
Date de la première version	13 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-021 du 12 avril 2011
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 XP Service Pack 3 ;
- Microsoft Excel 2002 Service Pack 3 ;
- Microsoft Office 2003 Service Pack 3 ;
- Microsoft Excel 2003 Service Pack 3 ;
- Microsoft Office 2007 Service Pack 2 ;
- Microsoft Excel 2007 Service Pack 2 ;
- Microsoft Office 2010 (édition 32-bit) ;
- Microsoft Excel 2010 (édition 32-bit) ;
- Microsoft Office 2010 (édition 64-bit) ;
- Microsoft Excel 2010 (édition 64-bit) ;
- Microsoft Office pour Mac ;
- Microsoft Office 2004 pour Mac ;

- Microsoft Office 2008 pour Mac ;
- Microsoft Office pour Mac 2011 ;
- Convertisseur de fichiers Open XML pour Mac ;
- Microsoft Excel Viewer Service Pack 2 ;
- Microsoft Office Compatibility Pack pour les fichiers au format Word, Excel, et PowerPoint 2007 Service Pack 2.

### 3 Résumé

Plusieurs vulnérabilités présentes dans Microsoft Excel permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

### 4 Description

Plusieurs vulnérabilités sont présentes dans le tableur Microsoft Excel. Elles permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire à distance via un fichier xls construit de façon particulière.

### 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 MS11-021 du 12 avril 2011 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-021.mspx>  
<http://www.microsoft.com/technet/security/Bulletin/MS11-021.mspx>
- Référence CVE CVE-2011-0097 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0097>
- Référence CVE CVE-2011-0098 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0098>
- Référence CVE CVE-2011-0101 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0101>
- Référence CVE CVE-2011-0103 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0103>
- Référence CVE CVE-2011-0104 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0104>
- Référence CVE CVE-2011-0105 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0105>
- Référence CVE CVE-2011-0978 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0978>
- Référence CVE CVE-2011-0979 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0979>
- Référence CVE CVE-2011-0980 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0980>

### Gestion détaillée du document

13 avril 2011 version initiale.