Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 12 mars 2008
N° CERTA-2008-AVI-125

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Microsoft Excel

Gestion du document

Référence	CERTA-2008-AVI-125
Titre	Multiples vulnérabilités dans Microsoft Excel
Date de la première version	12 mars 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-014 du 11 mars 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 ;
- déni de service à distance.

2 Systèmes affectés

- Microsoft Office 2000 Service Pack 3 ;
- Microsoft Office XP Service Pack 3 ;
- Microsoft Office 2003 Service Pack 2 ;
- Microsoft Office 2007 ;
- Microsoft Office Excel Viewer 2003 ;
- Pack de Compatibilité Microsoft Office pour les formats de fichiers Word, Excel et PowerPoint 2007 ;
- Microsoft Office 2004 pour Mac ;
- Microsoft Office 2008 pour Mac.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans l'application Microsoft Excel. L'une d'elles a fait l'objet en janvier 2008 de l'alerte CERTA-2008-ALE-003. Elles permettraient à une personne malveillante les exploitant via un fichier Excel spécialement construit 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 de bureautique Microsoft Excel.

- l'application ne manipulerait pas convenablement les macros à l'ouverture de fichiers Excel. Cette vulnérabilité a fait l'objet de l'alerte CERTA-2008-ALE-003 ;
- l'application ne contrôlerait pas correctement les données des fichiers Excel lorsqu'ils sont chargés en mémoire ;
- l'application ne vérifierait pas correctement les données de fichiers qui sont importés ;
- l'application ne manipulerait pas correctement des informations liées à un enregistrement STYLE à l'ouverture d'un fichier ;
- l'application ne validerait pas correctement des valeurs pour la mise en forme conditionnelle.

L'exploitation de ces vulnérabilités permettrait à une personne malveillante d'exécuter des commandes arbitraires sur le système vulnérable sur lequel un document spécifiquement construit serait ouvert.

Des codes d'exploitation concernant certaines de ces vulnérabilités circulent actuellement sur l'Internet.

5 Solution

Se référer au bulletin de sécurité MS08-014 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Document du CERTA CERTA-2008-ALE-003 du 16 mars 2008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-003/index.html
- Bulletin de sécurité Microsoft MS08-014 du 11 mars 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-014.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS08-014.mspx
- Référence CVE CVE-2008-0081 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0081
- Référence CVE CVE-2008-0111 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0111
- Référence CVE CVE-2008-0112 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0112
- Référence CVE CVE-2008-0114 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0114
- Référence CVE CVE-2008-0115 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0115
- Référence CVE CVE-2008-0116 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0116
- Référence CVE CVE-2008-0117 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0117

Gestion détaillée du document

12 mars 2008 version initiale.