Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 avril 2011
N° CERTA-2011-AVI-206

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft Office

Gestion du document

Référence	CERTA-2011-AVI-206
Titre	Vulnérabilités dans Microsoft Office
Date de la première version	13 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-023 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.

2 Systèmes affectés

- *Microsoft Office XP* Service Pack 3 ;
- *Microsoft Office 2003* Service Pack 3 ;
- *Microsoft Office 2007* Service Pack 2 ;
- *Microsoft Office 2004 pour Mac* ;
- *Microsoft Office 2008 pour Mac* ;
- *Convertisseur de formats de fichier Open XML pour Mac*.

3 Résumé

Deux vulnérabilités dans *Microsoft Office* permettent l'exécution de code arbitraire à distance.

4 Description

Deux vulnérabilités ont été découvertes dans *Microsoft Office* :

- une faille est liée à la façon dont sont chargées les bibliothèques dynamiques (CVE-2011-0107) ;
- lors du traitement d'un fichier *Office* contenant des objets graphiques, les structures de données de déréférencement ne sont pas correctement gérées (CVE-2011-0977).

L'exploitation de ces vulnérabilités permet l'exécution de code arbitraire à distance.

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 MS11-023 du 12 avril 2011 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS11-023.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS11-023.mspx
- Référence CVE CVE-2011-0107 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0107
- Référence CVE CVE-2011-0977 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0977

Gestion détaillée du document

13 avril 2011 version initiale.