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 juillet 2006
N° CERTA-2006-AVI-284

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de certains filtres de Microsoft Office

Gestion du document

Référence	CERTA-2006-AVI-284
Titre	Vulnérabilités de certains filtres de Microsoft Office
Date de la première version	12 juillet 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Microsoft du 11 juillet 2006
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 2003 Service Pack 1 et Service Pack 2 ;
- Microsoft Office XP Service Pack 3 ;
- Microsoft Office 2000 Service Pack 3 ;
- Microsoft Project 2002 ;
- Microsoft Project 2000 ;
- Microsoft Works Suites : 2004, 2005 et 2006.

Les visionneuses Microsoft Office, ainsi que Microsoft Office 2004 et Microsoft Office v. X pour MacOS ne sont pas concernées.

3 Description

Deux vulnérabilités ont été identifiées dans Microsoft Office. Elles concernent le filtrage de certains fichiers :

- la première vise le format `PNG`. Microsoft Office ne vérifie pas correctement l'allocation de l'espace mémoire. Une personne malveillante peut donc construire un fichier `.PNG` mal formé exploitant cette vulnérabilité, dans le but d'exécuter des commandes arbitraires sur le système vulnérable, quand l'utilisateur ouvrira ce fichier via Microsoft Office.
- la seconde vise le format `GIF`. Microsoft Office ne vérifie pas correctement l'allocation de l'espace mémoire lorsqu'il ouvre un fichier GIF. Un utilisateur malveillant peut construire un fichier spécial contenant une chaîne de caractères mal formée, afin d'exécuter du code arbitraire sur le système affecté.

4 Solution

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

5 Documentation

- Bulletin de sécurité Microsoft MS06-039 du 11 juillet 2006 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS06-039.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS06-039.mspx
- Référence CVE CVE-2006-0033 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0033

Gestion détaillée du document

12 juillet 2006 version initiale.