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-286

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités dans Microsoft Office

Gestion du document

Référence	CERTA-2006-AVI-286
Titre	Plusieurs vulnérabilités dans les logiciels Microsoft
Date de la première version	12 juillet 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft (MS06-038)
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 2003 Service Pack 1 ;
- Microsoft Office 2003 Service Pack 2 ;
- Microsoft Office XP Service Pack 3 ;
- Microsoft Office 2000 Service Pack 3 ;
- Microsoft Project 2002 Service Pack 2 ;
- Microsoft Visio 2002 Service Pack 2 ;
- Microsoft Project 2000 Service Release 1 ;
- Microsoft Office 2004 pour Mac ;
- Microsoft Office version X pour Mac.

3 Résumé

Plusieurs vulnérabilités présentes dans les logiciels Microsoft peuvent être utilisées par un utilisateur mal intentionné pour exécuter du code arbitraire sur un système ayant un des logiciels vulnénrables.

4 Description

- Une vulnérabilité dans le traitement de certains fichiers Microsoft Office peut être exploitée par un utilisateur mal intentionné pour exécuter du code arbitraire à partir d'un fichier spécialement construit (CVE-2006-1316) ;
- une vulnérabilité dans le traitement des chaînes comprises dans un fichier Microsoft Office peut être exploitée par un utilisateur mal intentionné pour exécuter du code arbitraire à distance (CVE-2006-1540) ;
- une vulnérabilité présente sur les propriétés d'un fichier Microsoft Office peut être exploitée par un utilisateur mal intentionné pour exécuter du code arbitraire à distance via un fichier spécialement construit (CVE-2006-2389).

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 MS06-038 du 11 juillet 2006 :
  http://www.microsoft.com/technet/security/Bulletin/MS06-038.mspx
  http://www.microsoft.com/france/technet/security/Bulletin/MS06-038.mspx
- Référence CVE CVE-2006-1316 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1316
- Référence CVE CVE-2006-1540 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1540
- Référence CVE CVE-2006-2389 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2389

Gestion détaillée du document

12 juillet 2006 version initiale.