



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-285

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-2006-AVI-285>

Gestion du document

Référence	CERTA-2006-AVI-285
Titre	Multiples vulnérabilités dans Microsoft Excel
Date de la première version	12 juillet 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-037
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 Office 2004 pour Mac ;
- Microsoft Office version X pour Mac.

3 Résumé

Plusieurs vulnérabilités sont présentes dans Microsoft Excel. Certaines de ces vulnérabilités peuvent être exploitées par un utilisateur distant pour exécuter du code arbitraire sur le système ayant la version vulnérable de ce logiciel.

4 Description

Huit vulnérabilités sont présentes dans le logiciel Microsoft Excel :

- Deux vulnérabilités existent dans les enregistrements *SELECTION* (CVE-2006-1301 et CVE-2006-1302). Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné à partir d'un enregistrement *SELECTION* dans un fichier Excel pour exécuter du code arbitraire sur le poste d'un utilisateur ouvrant le fichier spécialement construit.
- Une vulnérabilité existe dans les enregistrements *COLINFO* (CVE-2006-1304). Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné à partir d'un enregistrement *COLINFO* dans un fichier Excel pour exécuter du code arbitraire sur le poste d'un utilisateur ouvrant le fichier spécialement construit.
- Une vulnérabilité existe dans les enregistrements *OBJECT* (CVE-2006-1306). Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné à partir d'un enregistrement *OBJECT* dans un fichier Excel pour exécuter du code arbitraire sur le poste d'un utilisateur ouvrant le fichier spécialement construit.
- Une vulnérabilité existe dans les enregistrements *FNGROUPCOUNT* (CVE-2006-1308). Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné à partir d'un enregistrement *FNGROUPCOUNT* dans un fichier Excel pour exécuter du code arbitraire sur le poste d'un utilisateur ouvrant le fichier spécialement construit.
- Une vulnérabilité existe dans les enregistrements *LABEL* (CVE-2006-1309). Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné à partir d'un enregistrement *LABEL* dans un fichier Excel malveillant pour exécuter du code arbitraire sur le poste d'un utilisateur ouvrant le fichier malicieusement construit.
- Les deux dernières vulnérabilités présentes sur Excel peuvent être exploitées par un utilisateur mal intentionné à partir d'un fichier Excel malveillant (CVE-2006-2388 CVE-2006-3059). La dernière de ces vulnérabilités a fait l'objet d'une alerte au CERTA le 16 juin 2006.

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 MS06-037 du 11 juillet 2006 :
<http://www.microsoft.com/technet/security/Bulletin/MS06-037.msp>
<http://www.microsoft.com/france/technet/security/Bulletin/MS06-037.msp>
- Bulletin d'alerte du CERTA CERTA-2006-ALE-007 du 16 juin 2006 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-ALE-007/index.html>
- Référence CVE CVE-2006-1301 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1301>
- Référence CVE CVE-2006-1302 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1302>
- Référence CVE CVE-2006-1304 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1304>
- Référence CVE CVE-2006-1306 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1306>
- Référence CVE CVE-2006-1308 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1308>
- Référence CVE CVE-2006-1309 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1309>
- Référence CVE CVE-2006-2388 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2388>
- Référence CVE CVE-2006-3059 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3059>

Gestion détaillée du document

12 juillet 2006 version initiale.