



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 novembre 2010
N° CERTA-2010-AVI-543

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Microsoft Office

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-2010-AVI-543>

Gestion du document

Référence	CERTA-2010-AVI-543
Titre	Vulnérabilités dans Microsoft Office
Date de la première version	10 novembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-087 du 09 novembre 2010
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.

2 Systèmes affectés

- Microsoft Office XP SP3, 2003 SP3, 2007 SP2 et 2010 ;
- Microsoft Office pour Mac 2004, 2008 et 2011 ;
- Open XML File Format Converter pour Mac.

3 Résumé

Plusieurs vulnérabilités dans Microsoft Office permettent à un utilisateur malveillant d'exécuter du code avec les droits de l'utilisateur connecté.

4 Description

Plusieurs vulnérabilités dans Microsoft Office permettent à un utilisateur malveillant d'exécuter du code avec les droits de l'utilisateur connecté :

- une possibilité de débordement de mémoire dans le traitement des fichiers au format RTF est exploitable au moyen d'un fichier spécialement conçu ;
- des corruptions de mémoire dans les traitements de dessin et d'objets graphiques sont exploitables au moyen de fichiers Office spécialement construits ;
- la gestion d'une violation d'accès est également exploitable en utilisant un fichier Office spécialement conçu ;
- l'ordre de recherche des bibliothèques (DLL) est utilisable pour substituer une bibliothèque malveillante.

5 Solution

À la date du 10 novembre 2010, les correctifs pour Microsoft Office pour Mac 2004 et 2008 et pour Open XML File Format Converter ne sont pas encore disponibles.

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

6 Documentation

- Bulletin de sécurité Microsoft MS10-087 du 09 novembre 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-087.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-087.msp>
- Référence CVE CVE-2010-3333 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333>
- Référence CVE CVE-2010-3334 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3334>
- Référence CVE CVE-2010-3335 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3335>
- Référence CVE CVE-2010-3336 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3336>
- Référence CVE CVE-2010-3337 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3337>

Gestion détaillée du document

10 novembre 2010 version initiale.