



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 15 décembre 2010  
N° CERTA-2010-AVI-608

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-608>

---

### Gestion du document

Référence	CERTA-2010-AVI-608
Titre	Vulnérabilités dans Microsoft Office
Date de la première version	15 décembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-105 du 14 décembre 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 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 2010 éditions 32 bits et 64 bits ;
- Pack de conversion Microsoft Office ;
- Microsoft Works 9.

## 3 Résumé

Plusieurs vulnérabilités découvertes dans Microsoft Office permettent à un utilisateur distant malintentionné d'exécuter du code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités présentes dans les convertisseurs d'images aux formats TIFF, CGM, PICT et FlashPix de Microsoft Office ont été corrigées. Ces vulnérabilités peuvent être exploitées par une personne malveillante afin d'exécuter du code arbitraire à distance au moyen d'un document Microsoft Office spécialement construit.

## 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 MS10-105 du 14 décembre 2010 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-105.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS10-105.msp>
- Référence CVE CVE-2010-3945 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3945>
- Référence CVE CVE-2010-3946 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3946>
- Référence CVE CVE-2010-3947 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3947>
- Référence CVE CVE-2010-3949 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3949>
- Référence CVE CVE-2010-3950 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3950>
- Référence CVE CVE-2010-3951 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3951>
- Référence CVE CVE-2010-3952 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3952>

## Gestion détaillée du document

15 décembre 2010 version initiale.