

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités multiples d'OpenOffice

---

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-2007-AVI-405>

---

### Gestion du document

Référence	CERTA-2007-AVI-405
Titre	Vulnérabilités multiples d'OpenOffice
Date de la première version	18 septembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDefense 593 du 17 septembre 2007
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- la version 2.0.4 ainsi que toutes celles antérieures à 2.3.

## 3 Résumé

De multiples vulnérabilités ont été identifiées dans l'application bureautique OpenOffice. Elles concernent l'interprétation de fichiers au format TIFF. L'exploitation de ces dernières permettrait à une personne malveillante d'exécuter du code arbitraire sur le système ayant une version vulnérable.

## 4 Description

De multiples vulnérabilités ont été identifiées dans l'application bureautique OpenOffice. Elles concernent l'interprétation de fichiers au format TIFF. Il serait possible de tromper la taille de la mémoire à attribuer, et provoquer ainsi un débordement d'entier et de la pile.

Une personne pourrait exploiter l'une de ces vulnérabilités au moyen d'un fichier spécialement construit. Son ouverture par OpenOffice permettrait ainsi d'exécuter du code arbitraire sur le système ayant une version vulnérable.

## **5 Solution**

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

## **6 Documentation**

- Annonce de sécurité publiée sur le site du projet OpenOffice le 18 septembre 2007 :  
<http://www.openoffice.org/security/cves/CVE-2007-2834.html>
- Bulletin de sécurité RedHat RHSA-2007:0848 du 18 septembre 2007 :  
<http://rhn.redhat.com/errata/RHSA-2007-0848.html>
- Bulletin de sécurité 593 d'iDefense du 17 septembre 2007 :  
<http://labs.iddefense.com/intelligence/vulnerabilities/display?id=593>
- Référence CVE CVE-2007-2834 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2834>

## **Gestion détaillée du document**

**18 septembre 2007** version initiale.