

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans OpenOffice.org

---

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-136>

---

## Gestion du document

Référence	CERTA-2007-AVI-136-002
Titre	Multiples vulnérabilités dans OpenOffice.org
Date de la première version	21 mars 2007
Date de la dernière version	02 avril 2007
Source(s)	Bulletin de sécurité Debian DSA-1270 du 20 mars 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.

## 2 Systèmes affectés

- OpenOffice.org versions 1.0.3.1 et antérieures ;
- OpenOffice.org versions 1.1.5 et antérieures ;
- OpenOffice.org versions 2.1.0 et antérieures.

## 3 Résumé

De multiples vulnérabilités présentes dans OpenOffice.org permettent à un utilisateur distant d'exécuter du code arbitraire.

## 4 Description

Trois vulnérabilités sont présentent dans OpenOffice.org :

- la première est due au fait que OpenOffice.org embarque dans son code la bibliothèque de fonctions

libwpd mettant en œuvre le support des fichiers WordPerfect dans OpenOffice.org. Or, cette bibliothèque de fonction est vulnérable et permet l'exécution de code arbitraire (CERTA-2007-AVI-135) ;

- la deuxième vulnérabilité concerne le composant *tableur* de OpenOffice.org qui comporte une faille de type débordement de mémoire permettant l'exécution de code arbitraire ;
- la dernière vulnérabilité est, quant à elle, due à un manque de contrôle des paramètres passés en ligne de commande à OpenOffice.org. Ceci permet à un utilisateur malintentionné d'exécuter du code arbitraire à distance par le biais d'un lien construit de façon particulière.

## 5 Solution

La version 2.2 corrige les problèmes.

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

## 6 Documentation

- Bulletin de sécurité OpenOffice relatif à la référence CVE CVE-2007-0002 :  
<http://www.openoffice.org/security/CVE-2007-2.html>
- Bulletin de sécurité OpenOffice relatif à la référence CVE CVE-2007-0238 :  
<http://www.openoffice.org/security/CVE-2007-0238.html>
- Bulletin de sécurité OpenOffice relatif à la référence CVE CVE-2007-0239 :  
<http://www.openoffice.org/security/CVE-2007-0239.html>
- Avis CERTA-2007-AVI-135 du 21 mars 2007 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-135/index.html>
- Bulletin de sécurité Debian DSA-1268 du 17 mars 2007 :  
<http://www.debian.org/security/dsa-1268>
- Bulletin de sécurité Debian DSA-1270 du 20 mars 2007 :  
<http://www.debian.org/security/dsa-1270>
- Bulletin de sécurité Red Hat RHSA-2007:0033 du 22 mars 2007 :  
<http://rhn.redhat.com/errata/RHSA-2007-0033.html>
- Bulletin de sécurité SuSE SUSE-SA:2007:023 du 21 mars 2007 :  
<http://lists.suse.com/archive/suse-security-announce/2007-Mar/0007.html>
- Bulletin de sécurité Ubuntu USN-437-1 du 19 mars 2007 :  
<http://www.ubuntu.com/usn/usn-437-1>
- Bulletin de sécurité Ubuntu USN-444-1 du 27 mars 2007 :  
<http://www.ubuntu.com/usn/usn-444-1>
- Référence CVE CVE-2007-0002 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0002>
- Référence CVE CVE-2007-0238 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0238>
- Référence CVE CVE-2007-0239 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0239>

## Gestion détaillée du document

**21 mars 2007** version initiale.

**27 mars 2007** ajout des références aux bulletins de sécurité Debian, Red Hat, Ubuntu.

**28 mars 2007** ajout de référence au bulletin de sécurité Ubuntu.

**02 avril 2007** ajout des références aux bulletins de sécurité OpenOffice.