



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 juin 2007
N° CERTA-2007-AVI-264-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans 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-264>

Gestion du document

Référence	CERTA-2007-AVI-264-001
Titre	Vulnérabilité dans OpenOffice
Date de la première version	15 juin 2007
Date de la dernière version	25 juin 2007
Source(s)	
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.

2 Systèmes affectés

- OpenOffice versions 2.2.0 et antérieures ;
- StarOffice 7 Office Suite ;
- StarOffice 6.0 Office Suite ;
- StarOffice 8 Office Suite.

3 Résumé

Une vulnérabilité découverte dans OpenOffice.org pourrait être exploitée, via un fichier `rtf` malicieusement construit, pour réaliser un déni de service ou exécuter du code arbitraire sur la machine vulnérable. Cette vulnérabilité est due à un débordement de tampon dans la fonction `SwRTFParser::ReadPrtdata()`.

4 Solution

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

5 Documentation

- Mise à jour d'OpenOffice (version 2.2.1) :
<http://download.openoffice.org/index.html>
- Référence CVE CVE-2007-0245 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0245>
- Référence CVE CVE-2007-2754 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2754>
- Bulletin de sécurité Sun Microsystems 102917 du 15 juin 2007 :
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-102917-1>

Gestion détaillée du document

15 juin 2007 version initiale.

25 juin 2007 ajout de la référence à StarOffice.