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 mai 2005
N° CERTA-2005-AVI-147-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans OpenOffice

Gestion du document

Référence	CERTA-2005-AVI-147-002
Titre	Vulnérabilité dans OpenOffice
Date de la première version	18 avril 2005
Date de la dernière version	10 mai 2005
Source(s)	Bulletin de sécurité OpenOffice #46388
Pièce(s) jointe(s)	

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

OpenOffice 1.1.4 et versions antérieures.

3 Résumé

Une vulnérabilité découverte dans OpenOffice permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

4 Description

OpenOffice est une suite bureautique.

Une vulnérabilité de type débordement de mémoire est présente dans la fonction `StgCompObjStream::Load()` qui permet d'interpréter l'entête des fichiers `.doc` (Microsoft Word). Un utilisateur mal intentionné peut exécuter du code arbitraire, au moyen d'un fichier `.doc` malicieusement 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 OpenOffice #46388 du 13 avril 2005 :
  http://www.openoffice.org/issues/show_bug.cgi?id=46388
- Bulletin de sécurité Gentoo GLSA 200504-13 / OpenOffice du 15 avril 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200504-13.xml
- Mise à jour de sécurité Fedora Core 2 pour OpenOffice du 14 avril 2005 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
- Mise à jour de sécurité Fedora Core 3 pour OpenOffice du 14 avril 2005 :
  http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/
- Bulletin de sécurité FreeBSD pour OpenOffice du 13 avril 2005 :
  http://www.vuxml.org/freebsd/pkg-pl-openoffice.html
- Bulletin de sécurité SUSE SUSE-SA:2005:025 du 19 avril 2005 :
  http://www.novell.com/linux/security/advisories/2005_25_openoffice_org.html
- Bulletin de sécurité Mandriva MDKSA-2005:082 du 06 mai 2005 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2005:082
- Référence CVE CAN-2005-0941 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0941

Gestion détaillée du document

18 avril 2005 version initiale.
21 avril 2005 ajout référence au bulletin de sécurité SuSE. Ajout référence CVE.
10 mai 2005 ajout référence au bulletin de sécurité Mandriva.