

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans KOffice/KWord

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-2005-AVI-444>

Gestion du document

Référence	CERTA-2005-AVI-444
Titre	Vulnérabilité dans KOffice/KWord
Date de la première version	08 novembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité SuSE du 04 novembre 2005
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

KOffice 1.x.

3 Résumé

Une vulnérabilité dans KOffice permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

KOffice est une suite bureautique pour KDE.

Le logiciel de traitement de texte KWord pour KOffice présente une vulnérabilité de type débordement de mémoire. Cette vulnérabilité peut être exploitée à distance afin d'exécuter du code arbitraire au moyen d'un fichier au format RTF malicieusement construit.

5 Solution

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

6 Documentation

- Bulletin de sécurité KOffice du 11 octobre 2005 :
<http://www.koffice.org/security/advisory-20051011-1.txt>
- Bulletin de sécurité Gentoo GLSA 200510-12 du 14 octobre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200510-12.xml>
- Bulletin de sécurité Debian DSA-872 du 26 octobre 2005 :
<http://www.debian.org/security/2005/dsa-872>
- Bulletin de sécurité Ubuntu USN-202 du 12 octobre 2005 :
<http://www.ubuntu.com/usn/usn-202-1>
- Mise à jour de sécurité Fedora Core 3 du 17 octobre 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Bulletin de sécurité SuSE SUSE-SR:2005:025 du 04 novembre 2005 :
<http://lists.suse.com/archive/suse-security-announce/2005-Nov/0001.html>
- Référence CVE CAN-2005-2971 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2971>

Gestion détaillée du document

08 novembre 2005 version initiale.