

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de libtiff

---

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-195>

---

### Gestion du document

Référence	CERTA-2005-AVI-195-004
Titre	Vulnérabilité de libtiff
Date de la première version	08 juin 2005
Date de la dernière version	27 février 2006
Source(s)	Bulletin de sécurité Gentoo GLSA 200505-07
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

Libtiff 3.7.2 et versions antérieures.

## 3 Description

Libtiff est une bibliothèque pour le traitement des images au format TIFF (Tag Image File Format).

Une vulnérabilité de type débordement de mémoire est présente dans la bibliothèque libtiff.

En incitant un utilisateur à visualiser une image au format TIFF habilement constituée, cette vulnérabilité peut être exploitée afin d'exécuter du code arbitraire via une application utilisant la bibliothèque vulnérable.

## 4 Solution

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

## 5 Documentation

- Bulletin de sécurité Gentoo GLSA 200505-07 du 10 mai 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200505-07.xml>
- Bulletin de sécurité SUSE SUSE-SR:2005:014 du 07 juin 2005 :  
[http://www.novell.com/linux/security/advisories/2005\\_14\\_sr.html](http://www.novell.com/linux/security/advisories/2005_14_sr.html)
- Bulletin de sécurité Debian DSA-755 du 13 juillet 2005 :  
<http://www.debian.org/security/2005/dsa-755>
- Bulletin de sécurité FreeBSD pour tiff et linux-tiff du 30 juillet 2005 :  
<http://www.vuxml.org/freebsd/pkg-tiff.html>  
<http://www.vuxml.org/freebsd/pkg-linux-tiff.html>
- Bulletin de sécurité SCO SCOSA-2006.3 du 03 janvier 2006 :  
<ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2006.3/SCOSA-2006.3.txt>
- Bulletin de sécurité Mandriva MDKSA-2006:042 du 17 février 2006 :  
<http://frontal2.mandriva.com/security/advisories?name=MDKSA-2006:042>
- Référence CVE CAN-2005-1544 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1544>

### Gestion détaillée du document

**08 juin 2005** version initiale.

**13 juillet 2005** ajout de la référence au bulletin de sécurité Debian.

**01 août 2005** ajout de la référence au bulletin de sécurité FreeBSD.

**05 janvier 2006** ajout de la référence au bulletin de sécurité SCO.

**27 février 2006** ajout de la référence au bulletin de sécurité Mandriva.