

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Tcl/Tk

---

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-2008-AVI-240>

---

### Gestion du document

Référence	CERTA-2008-AVI-240
Titre	Vulnérabilité dans Tcl/Tk
Date de la première version	13 mai 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Sun 237465 du mardi 6 mai 2008
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 à distance.

## 2 Systèmes affectés

Les versions antérieures à la 8.5.1.

## 3 Résumé

Une vulnérabilité affectant la bibliothèque Tcl/Tk lors du traitement des images au format GIF a été corrigée.

## 4 Description

Une fonction de la bibliothèque Tcl/Tk vulnérable à un dépassement de mémoire permet à un utilisateur malveillant d'exécuter du code arbitraire à distance à l'aide d'une image spécifiquement réalisée.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Debian DSA 1490 du 10 février 2008 :  
<http://www.debian.org/security/2008/dsa-1490>
- Bulletin de sécurité Debian DSA 1491 du 10 février 2008 :  
<http://www.debian.org/security/2008/dsa-1491>
- Mise à jour de sécurité Fedora 2008-1122,2008-1131,2008-1323 et 2008-1384 7 février 2008 :  
<http://www.redhat.com/archives/fedora-package-announce/2008-February/msg00193.html>  
<http://www.redhat.com/archives/fedora-package-announce/2008-February/msg00132.html>  
<http://www.redhat.com/archives/fedora-package-announce/2008-February/msg00115.html>  
<http://www.redhat.com/archives/fedora-package-announce/2008-February/msg00205.html>
- Bulletin de sécurité Mandriva MDVSA-2008:041 du 07 février 2008 :  
<http://www.mandriva.com/archives/security/advisories>
- Bulletin de sécurité RedHat RHSA-2008:0134 du 21 février 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0134.html>
- Bulletin de sécurité RedHat RHSA-2008:0135 du 21 février 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0135.html>
- Bulletin de sécurité RedHat RHSA-2008:0136 du 21 février 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0136.html>
- Bulletin de sécurité Sun Solaris #237465 du 06 mai 2008 :  
<http://sunsolve.sun.com/search/document.do?assetkey=1-26-237465-1>
- Référence CVE CVE-2008-0553 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0553>

## Gestion détaillée du document

**13 mai 2008** version initiale.