



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 02 août 2006  
N° CERTA-2006-AVI-319

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans la librairie libgd

---

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-2006-AVI-319>

---

### Gestion du document

Référence	CERTA-2006-AVI-319
Titre	Vulnérabilité dans la bibliothèque libgd
Date de la première version	02 août 2006
Date de la dernière version	–
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

Déni de service à distance.

## 2 Systèmes affectés

libgd 2.x.

## 3 Résumé

Une vulnérabilité découverte dans la bibliothèque libgd peut être exploitée par un utilisateur mal intentionné afin de provoquer un déni de service à distance.

## 4 Description

Une vulnérabilité dans la fonction `gdImageCreateFromGifPtr()` peut être exploitée au moyen d'un fichier `gif` spécialement construit afin de provoquer un déni de service en consommant les ressources processeur. Cette vulnérabilité affecte toutes les applications et les services faisant appels à la bibliothèque vulnérable.

## 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 1117 du 21 juillet 2006 :  
<http://www.debian.org/security/2006/dsa-1117/>
- Bulletin de sécurité Mandriva MDKSA-2006:112 du 27 juin 2006 :  
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:112>
- Bulletin de sécurité Ubuntu USN-298-1 du 13 juin 2006 :  
<http://www.ubuntulinux.org/usn/usn-298-1>
- Référence CVE CVE-2006-2906 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2906>

## Gestion détaillée du document

**02 août 2006** version initiale.