

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans la bibliothèque libgda

---

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-441>

---

### Gestion du document

Référence	CERTA-2005-AVI-441
Titre	Multiples vulnérabilités dans la bibliothèque libgda
Date de la première version	07 novembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Gentoo GLSA 200511-01 du 02 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

GNOME-DB 1.x.

## 3 Résumé

Deux vulnérabilités découvertes dans la bibliothèque libgda permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

## 4 Description

libgda est une bibliothèque notamment utilisée par l'application GNOME-DB.

Deux vulnérabilités de type "chaîne de formats" présentes dans les fonctions `gda_log_error` et `gda_log_messages` peuvent être exploitées par un individu distant mal intentionné afin d'exécuter du code arbitraire.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Gentoo GLSA 200511-01 du 02 novembre 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200511-01.xml>
- Bulletin de sécurité Debian DSA-871 du 25 octobre 2005 :  
<http://www.debian.org/security/2005/dsa-871>
- Bulletin de sécurité Ubuntu USN-212-1 du 28 octobre 2005 :  
<http://www.ubuntu.com/usn/usn-212-1>
- Référence CVE CAN-2005-2958 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2758>

## Gestion détaillée du document

**07 novembre 2005** version initiale.