



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 21 septembre 2007  
N° CERTA-2007-AVI-413

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans libvorbis

---

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-2007-AVI-413>

---

### Gestion du document

Référence	CERTA-2007-AVI-413
Titre	Vulnérabilités dans libvorbis
Date de la première version	21 septembre 2007
Date de la dernière version	–
Source(s)	Annonce de mise à jour du projet libvorbis
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- libvorbis, pour les versions antérieures à 1.1.3.

## 3 Description

Plusieurs vulnérabilités ont été identifiées dans la bibliothèque libvorbis, dédiée au format multimédia Ogg Vorbis. Elles peuvent être exploitées par une personne malveillante sous la forme de fichier .ogg spécialement construits, afin de perturber ou exécuter des commandes sur le système ayant une version vulnérable.

## 4 Solution

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

## 5 Documentation

- Page officiel du projet libvorbis :  
<http://xiph.org/vorbis/>
- Bulletin de sécurité iSec Partners du 26 juillet 2007 :  
<http://www.isecpartners.com/advisories/2007-003-libvorbis.txt>
- Référence CVE CVE-2007-4029 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4029>
- Référence CVE CVE-2007-4065 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4065>
- Référence CVE CVE-2007-4066 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4066>

### Gestion détaillée du document

21 septembre 2007 version initiale.