



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 04 janvier 2005  
N° CERTA-2004-AVI-417-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité dans mpg123**

---

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-2004-AVI-417>

---

### Gestion du document

Référence	CERTA-2004-AVI-417-001
Titre	Vulnérabilité dans mpg123
Date de la première version	22 décembre 2004
Date de la dernière version	04 janvier 2005
Source(s)	Bulletin de sécurité Gentoo
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.

## 2 Systèmes affectés

mpg123 versions antérieures à la version 0.59.

## 3 Résumé

Une vulnérabilité présente dans mpg123 permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur le système utilisant une version vulnérable du lecteur.

## 4 Description

Un débordement de mémoire est présent dans la fonction chargée du traitement des listes de fichiers audio du lecteur audio mpg123.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité, via des listes de fichiers audio malicieusement construites, pour exécuter du code arbitraire sur le système ayant un lecteur vulnérable.

## 5 Contournement provisoire

Ne pas utiliser les listes de fichiers audio sur le lecteur mpg123.

## 6 Solution

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

## 7 Documentation

- Bulletin de sécurité Gentoo :  
<http://www.gentoo.org/security/en/glsa/glsa-200412-22.xml>
- Bulletin de sécurité FreeBSD "mpg123 – playlist processing buffer overflow vulnerability" du 03 janvier 2005 :  
<http://www.vuxml.org/freebsd/>
- Référence CVE CAN-2004-1284 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1284>

## Gestion détaillée du document

**22 décembre 2004** version initiale.

**04 janvier 2005** Ajout référence au bulletin de sécurité de FreeBSD. Correction erreur typo. dans le titre.