



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 25 août 2004  
N° CERTA-2004-AVI-277

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Xine

---

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-277>

---

### Gestion du document

Référence	CERTA-2004-AVI-277
Titre	Vulnérabilité de Xine
Date de la première version	25 août 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité open-security #6 du 08 août 2004
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

*xine-lib* versions 1-rc5 et antérieures.

## 3 Résumé

Une vulnérabilité de *Xine* permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur un système vulnérable.

## 4 Description

*Xine* est un lecteur multimédia pour les plates-formes Unix.

Une vulnérabilité de type débordement de mémoire a été découverte dans la gestion des entrées de type "vcd://".

Elle permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire avec les privilèges de l'utilisateur ayant lancé *Xine*.

Cette vulnérabilité peut-être exploitée par le biais d'un fichier *playlist* malicieusement construit.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité open-security #6 du 08 août 2004 :  
<http://www.open-security.org/advisories/6>
- Bulletin de sécurité Gentoo GLSA-200408-18 du 17 août 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200408-18.xml>
- Bulletin de sécurité FreeBSD pour xine du 23 août 2004 :  
<http://www.vuxml.org/freebsd/>

## Gestion détaillée du document

25 août 2004 version initiale.