

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de aRts

---

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-269>

---

### Gestion du document

Référence	CERTA-2006-AVI-269
Titre	Vulnérabilité de aRts
Date de la première version	29 juin 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité KDE du 14 juin 2006
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 ;
- élévation de privilèges.

## 2 Systèmes affectés

`artswrapper` du package `aRts`, avec le drapeau `setuid root` positionné, sous les noyaux Linux 2.6.0 ou versions supérieures.

## 3 Résumé

Une vulnérabilité dans le package `aRts` permet à un utilisateur mal intentionné d'élèver ses privilèges.

## 4 Description

`aRts` est un système modulaire de gestion des sons sous Linux, utilisé notamment par KDE.  
`artswrapper` est un binaire du package `aRts` permettant d'exécuter du code avec des privilèges élevés.  
Une vulnérabilité dans le binaire `artswrapper` permet à un utilisateur mal intentionné d'élèver ses privilèges au niveau de celui de `root`.

## 5 Contournement provisoire

Dans l'attente de l'application des correctifs, enlever le drapeau `setuid root` du binaire `artswrapper`.

## 6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Il est également possible d'appliquer les correctifs pour `aRtS` depuis les sources. Les correctifs se trouvent à cette adresse :

[ftp://ftp.kde.org/pub/kde/security\\_patches](ftp://ftp.kde.org/pub/kde/security_patches)

## 7 Documentation

- Bulletin de sécurité KDE du 14 juin 2006 :  
<http://www.kde.org/info/security/advisory-20060614-2.txt>
- Bulletin de sécurité Mandriva MDKSA-2006:107 du 20 juin 2006 :  
<http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:107>
- Bulletin de sécurité Gentoo GLSA-200606-22 du 22 juin 2006 :  
<http://www.gentoo.org/security/en/glsa/glsa-200606-22.xml>
- Référence CVE CVE-2006-2916 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2916>

## Gestion détaillée du document

**29 juin 2006** version initiale.