

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans KDM

---

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-2010-AVI-187>

---

### Gestion du document

Référence	CERTA-2010-AVI-187
Titre	Vulnérabilité dans KDM
Date de la première version	19 avril 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité KDE 20100413-1 du 13 avril 2010
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

Élévation de privilèges.

## 2 Systèmes affectés

Toutes les versions de KDE jusqu'à KDE SC 4.4.2 inclus.

## 3 Résumé

Une vulnérabilité dans KDM (*KDE Display Manager*) permet à une personne malintentionnée d'élever ses privilèges sur le système.

## 4 Description

Une vulnérabilité permet à un utilisateur de modifier les droits d'accès aux fichiers lorsque KDM crée sa *socket* de contrôle durant l'ouverture de session. Cette vulnérabilité permet, selon certaines conditions, d'exécuter du code arbitraire avec les droits de *root*.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité KDE 20100413-1 du 13 avril 2010 :  
<http://www.kde.org/info/security/advisory-20100413-1.txt>
- Référence CVE CVE-2010-0436 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0436>

## **Gestion détaillée du document**

**19 avril 2010** version initiale.