

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Konqueror

---

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-384>

---

### Gestion du document

Référence	CERTA-2007-AVI-384
Titre	Multiples vulnérabilités dans Konqueror
Date de la première version	30 août 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité KDE du 16 août 2007
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

Usurpation du contenu de la barre d'adresse.

## 2 Systèmes affectés

Konqueror versions 3.5.7 et antérieures.  
D'autres navigateurs utilisant le même moteur de rendu peuvent être affectés.

## 3 Résumé

De multiples vulnérabilités dans Konqueror permettent d'usurper le contenu de la barre d'adresse.

## 4 Description

Trois vulnérabilités dans Konqueror permettent à une personne malintentionnée d'usurper le contenu de la barre d'adresse de l'utilisateur, soit en insérant des espaces dans l'adresse réticulaire, ou en changeant la propriété `window.location` de manière répétée avec la fonction `JavaScript setInterval()`.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité KDE du 16 août 2007 :  
<http://www.kde.org/info/security/advisory-20070816-1.txt>
- Bulletin de sécurité Ubuntu USN 502-1 du 23 août 2007 :  
<http://www.ubuntu.com/usn/usn-502-1>
- Référence CVE CVE-2007-3820 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3820>
- Référence CVE CVE-2007-4224 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4224>
- Référence CVE CVE-2007-4225 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4225>

## Gestion détaillée du document

**30 août 2007** version initiale.