



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 novembre 2003  
N° CERTA-2003-AVI-193

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Opera

---

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-2003-AVI-193>

---

### Gestion du document

Référence	CERTA-2003-AVI-193
Titre	Vulnérabilité dans Opera
Date de la première version	14 novembre 2003
Date de la dernière version	–
Source(s)	–
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

Opera version 7.21 et antérieures.

## 3 Résumé

Deux vulnérabilités dans Opera permettent à un utilisateur mal intentionné d'exécuter du code arbitraire.

## 4 Description

Opera est un navigateur développé pour de nombreuses plate-formes. Deux vulnérabilités ont été identifiées :

- La première vulnérabilité concerne la gestion des fichiers de type `application/x-opera-skin` ;
- la seconde vulnérabilité concerne l'URI (Uniform Resource Identifier) `opera:` .

En combinant ces deux vulnérabilités, un utilisateur mal intentionné peut exécuter du code arbitraire.

## **5 Solution**

Mettre à jour Opera en version 7.22 :  
<http://www.opera.com/download/>

## **6 Documentation**

Site d'Opera :  
<http://www.opera.com>

## **Gestion détaillée du document**

**14 novembre 2003** version initiale.