

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-199>

Gestion du document

Référence	CERTA-2003-AVI-199
Titre	Vulnérabilité dans Opera
Date de la première version	25 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 à distance.

2 Systèmes affectés

Opera version 7.22 et versions antérieures.

3 Résumé

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

4 Description

Opera est un navigateur développé pour de nombreuses plate-formes. Deux vulnérabilités ont été identifiées :
– La première vulnérabilité est une traversée d'arborescence permettant de déposer un fichier dans un endroit arbitraire ;

- la seconde vulnérabilité concerne un débordement de mémoire dans le traitement des fichiers de type application/x-opera-skin.

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

5 Solution

Mettre à jour Opera en version 7.23 :
<http://www.opera.com/download/>

6 Documentation

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

Gestion détaillée du document

25 novembre 2003 version initiale.