



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 août 2008
N° CERTA-2008-AVI-426

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2008-AVI-426>

Gestion du document

Référence	CERTA-2008-AVI-426
Titre	Multiples vulnérabilités dans Opera
Date de la première version	20 août 2008
Date de la dernière version	–
Source(s)	Notes de version Opera 9.52
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 ;
- contournement de la politique de sécurité ;
- injection de code indirecte.

2 Systèmes affectés

Opera 9.51.

3 Résumé

De multiples vulnérabilités dans *Opera* permettent l'exécution de code arbitraire à distance, le contournement de la politique de sécurité et la réalisation d'attaques de type `cross-site scripting`.

4 Description

De multiples vulnérabilités ont été découvertes dans *Opera* :

- *Opera* peut être invoqué pour traiter certains protocoles. Dans certains cas, lorsqu'*Opera* est appelé par une application externe, une exécution de code arbitraire est possible ;
- des scripts sont capables de changer l'adresse de cadres de page qui viennent du même site. Une vulnérabilité dans ce mécanisme permet à un site de modifier l'adresse de cadres provenant d'autres sites ;
- des raccourcis et des commandes de menu peuvent être utilisés pour appeler des applications externes. Les paramètres passés à ces applications peuvent être incorrects, ce qui peut conduire à une exécution de code arbitraire ;
- des pages considérées comme non sûres peuvent charger dans un cadre du contenu provenant de sites considérés comme sûrs ;
- une vulnérabilité permet de créer des liens vers des fichiers locaux ;
- une vulnérabilité lors de l'inscription à des flux permet d'afficher une mauvaise adresse ;
- une injection de code indirecte est possible.

5 Solution

Mettre *Opera* à jour en version 9.52.

6 Documentation

- Notes de version Opera 9.52 :
<http://www.opera.com/docs/changelog/windows/952/>
- Bulletins de sécurité Opera :
<http://www.opera.com/support/search/view/892/>
<http://www.opera.com/support/search/view/893/>
<http://www.opera.com/support/search/view/894/>
<http://www.opera.com/support/search/view/895/>
<http://www.opera.com/support/search/view/896/>
<http://www.opera.com/support/search/view/897/>

Gestion détaillée du document

20 août 2008 version initiale.