

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : 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-2010-AVI-274>

---

### Gestion du document

Référence	CERTA-2010-AVI-274
Titre	Vulnérabilités dans Opera
Date de la première version	21 juin 2010
Date de la dernière version	–
Source(s)	Notes de la version 10.54 d'Opera pour Windows du 21 juin 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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

Opera versions 10.53 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités dans *Opera* permettent d'exécuter du code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités ont été découvertes dans *Opera*. Seuls les détails de l'une d'entre elles ont été dévoilés. Un problème dans la gestion de certaines polices de caractères par *Windows* permet une élévation de privilèges. Cette vulnérabilité a fait l'objet d'un correctif de *Microsoft* (voir avis CERTA-2010-AVI-244), mais est exploitable au travers d'*Opera* sur les systèmes non mis à jour, ce qui permet donc l'exécution de code arbitraire à distance. *Opera Software* a publié un correctif qui protège l'exploitation de cette vulnérabilité via le navigateur, même sur les systèmes non mis à jour.

## 5 Solution

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

## 6 Documentation

- Notes de la version 10.54 d'Opera pour Windows du 21 juin 2010 :  
<http://www.opera.com/docs/changelogs/windows/1054/>
- Bulletin de sécurité 954 d'Opera :  
<http://www.opera.com/support/kb/view/954/>
- Avis CERTA-2010-AVI-244 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-244/>
- Référence CVE CVE-2010-1255 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1255>

## Gestion détaillée du document

**21 juin 2010** version initiale.