



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 28 décembre 2007  
N° CERTA-2007-AVI-555-001

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-2007-AVI-555>

---

### Gestion du document

Référence	CERTA-2007-AVI-555-001
Titre	Multiples vulnérabilités dans Opera
Date de la première version	19 décembre 2007
Date de la dernière version	28 décembre 2007
Source(s)	Bulletin de sécurité Opera 875 Notes de version Opera 9.25
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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

Opera versions 9.24 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités dans *Opera* permettent d'exécuter du code arbitraire à distance, d'accéder en lecture à des zones de la mémoire ou de réaliser des attaques de type *cross-domain scripting*.

## 4 Description

Plusieurs vulnérabilités ont été découvertes dans *Opera* :

- une vulnérabilité dans le traitement des certificats TLS permet l'exécution de code arbitraire à distance ;
- une vulnérabilité dans le traitement des *bitmaps* permet d'accéder en lecture à des zones de la mémoire ;
- une vulnérabilité dans l'édition Rich Text permet de réaliser des attaques de type *cross-domain scripting* ;
- une vulnérabilité dans les modules peut être utilisée pour réaliser des attaques de type *cross-domain scripting*.

## 5 Solution

Mettre à jour *Opera* en version 9.25 (cf. section Documentation).

## 6 Documentation

- Version 9.25 d'Opera :  
<http://www.opera.com/>
- Bulletin de sécurité Opera 875 :  
<http://www.opera.com/support/search/view/875/>
- Notes de version Opera 9.25 :  
<http://www.opera.com/docs/changelogs/windows/925/#security>
- Référence CVE CVE-2007-6520 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6520>
- Référence CVE CVE-2007-6521 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6521>
- Référence CVE CVE-2007-6522 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6522>
- Référence CVE CVE-2007-6523 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6523>
- Référence CVE CVE-2007-6524 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6524>

## Gestion détaillée du document

**19 décembre 2007** version initiale.

**28 décembre 2007** ajout des références CVE associées.