

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Plusieurs vulnérabilités dans le navigateur 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-013>

---

### Gestion du document

Référence	CERTA-2007-AVI-013-001
Titre	Plusieurs vulnérabilités dans le navigateur Opera
Date de la première version	09 janvier 2007
Date de la dernière version	23 janvier 2007
Source(s)	Avis de sécurité Opera Software du 05 janvier 2007
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 ;
- déni de service à distance.

## 2 Systèmes affectés

Les versions du navigateur Opera antérieures à la 9.10.

## 3 Description

Deux vulnérabilités ont été identifiées dans le navigateur Web Opera.

La première concerne la manipulation par le navigateur des images au format JPG (pour *Joint Photographic Experts Group*). Il n'interpréterait pas correctement le marqueur DHT (Define Huffman Table(s)) d'une image, servant à la compression (ou décompression) de celle-ci. Un site compromis pourrait donc contenir sur une page une image JPG spécialement construite. La visite de cette page provoquerait sur le poste du visiteur un mauvais fonctionnement du navigateur, voire une exécution de code arbitraire.

La seconde concerne la manipulation par le navigateur des images au format SVG (pour *Scalable Vector Graphics*). Il ne vérifierait pas le paramètre passé à la fonction Javascript `createSVGTransformFromMatrix`.

Un site compromis pourrait donc contenir sur une page une image SVG spécialement construite. La visite de cette page via un navigateur ayant Javascript activé provoquerait sur le poste du visiteur l'exécution de code arbitraire avec les droits de ce dernier.

## 4 Solution

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

## 5 Documentation

- Avis de sécurité Opera Software 851 du 05 janvier 2007 :  
<http://www.opera.com/support/search/supsearch.dml?index=851>
- Avis de sécurité Opera Software 852 du 05 janvier 2007 :  
<http://www.opera.com/support/search/supsearch.dml?index=852>
- Avis de sécurité 457 d'iDefense du 05 janvier 2007 :  
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=457>
- Avis de sécurité 458 d'iDefense du 05 janvier 2007 :  
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=458>
- Documentation concernant le format JPEG en français :  
<https://kessel.ordrejedis.net/neo/mathsiPrInfo.pdf>
- Référence CVE CVE-2007-0126 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0126>
- Référence CVE CVE-2007-0127 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0127>
- Bulletin de sécurité Gentoo GLSA 200701-08 du 12 janvier 2007 :  
<http://security.gentoo.org/glsa-200701-08.xml>
- Bulletin de sécurité Suse SUSE-SA:2007:009 du 15 janvier 2007 :  
<http://lists.suse.com/archive/suse-security-announce/2007-Jan/0009.html>

## Gestion détaillée du document

**09 janvier 2007** version initiale.

**23 janvier 2007** ajout des références CVE, Gentoo et Suse.