

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du 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-324>

Gestion du document

Référence	CERTA-2007-AVI-324
Titre	Multiples vulnérabilités du navigateur Opera
Date de la première version	20 juillet 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité Opera #862, #863 et #864 du 19 juillet 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 ;
- usurpation d'adresse réticulaire.

2 Systèmes affectés

Opera versions 9.21 et antérieures.

3 Résumé

Plusieurs vulnérabilités dans le navigateur Opera permettent à un utilisateur distant d'exécuter du code arbitraire.

4 Description

Plusieurs vulnérabilités sont présentes dans le navigateur Opera :

- la première relative à la mise en œuvre du protocole de pair-à-pair BitTorrent est présente dans le navigateur Opera. L'exploitation de cette faille requiert que la victime clique sur un lien vers un fichier de

type BitTorrent construit de façon particulière puis enlève la référence au fichier correspondant dans le gestionnaire de téléchargement ;

- deux autres vulnérabilités concernent la possibilité pour un utilisateur malintentionné de faire afficher dans la barre d'adresse du navigateur une URL arbitraire.

5 Solution

La version 9.22 de Opera corrige le problème :

<http://www.opera.com/download/>

6 Documentation

Bulletin de sécurité Opera n°862 :

<http://www.opera.com/support/search/view/862>

Bulletin de sécurité Opera n°863 :

<http://www.opera.com/support/search/view/863>

Bulletin de sécurité Opera n°864 :

<http://www.opera.com/support/search/view/864>

Gestion détaillée du document

20 juillet 2007 version initiale.