

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-2010-AVI-384>

Gestion du document

Référence	CERTA-2010-AVI-384-001
Titre	Multiples vulnérabilités dans Opera
Date de la première version	13 août 2010
Date de la dernière version	17 août 2010
Source(s)	Note de version Opera 10.61 du 12 août 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 antérieures à 10.61.

3 Résumé

De multiples vulnérabilités ont été découvertes dans Opera. Elles permettent entre autres l'exécution de code arbitraire à distance.

4 Description

Quatre vulnérabilités ont été corrigées dans la dernière version d'Opera :

- le chargement d'un image animé au format PNG peut épuiser les ressources processeur ;
- certaines actions peuvent entraîner un débordement de tas lors de l'affichage d'un canevas HTML5 ;

- une erreur dans la gestion des onglets peut être utilisée par une personne malveillante pour tromper les utilisateurs et leur faire télécharger un exécutable sans qu'ils en aient conscience ;
- une erreur dans le traitement des flux d'informations RSS permet à une personne malveillante de forcer un utilisateur à s'abonner à un flux particulier.

5 Solution

La version 10.61 d'Opera remédie à ces vulnérabilités.

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

6 Documentation

- Note de version Opera 10.61 du 12 août 2010 :
<http://www.opera.com/docs/changelogs/windows/1061/>
- Bulletin de sécurité Opéra 966 :
<http://www.opera.com/support/kb/view/966/>
- Bulletin de sécurité Opéra 967 :
<http://www.opera.com/support/kb/view/967/>
- Bulletin de sécurité Opéra 968 :
<http://www.opera.com/support/kb/view/968/>
- Référence CVE CVE-2010-2576 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2576>
- Référence CVE CVE-2010-3019 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3019>
- Référence CVE CVE-2010-3020 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3020>
- Référence CVE CVE-2010-3021 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3021>

Gestion détaillée du document

13 août 2010 version initiale.

17 août 2010 ajout de la vulnérabilité PNG et de trois références CVE.