

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-498>

Gestion du document

Référence	CERTA-2010-AVI-498-001
Titre	Multiples vulnérabilités dans Opera
Date de la première version	13 octobre 2010
Date de la dernière version	27 octobre 2010
Source(s)	Note de mise à jour Opera publiée le 12 octobre 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

- Contournement de la politique de sécurité ;
- injection de code indirecte à distance.

2 Systèmes affectés

Opera versions antérieures à 10.63.

3 Résumé

Une mise à jour du navigateur Web Opera corrige de multiples vulnérabilités, permettant notamment le contournement de politique de sécurité, la conduite d'attaques de type "injection de code indirecte".

4 Description

De multiples vulnérabilités ont été reportées sur le navigateur Web Opera. Un utilisateur malveillant peut, en exploitant ces vulnérabilités, conduire des attaques de type injection de code indirecte à distance, modifier l'affichage de l'URL visitée (usurpation d'affichage), faire exécuter des scripts hors de leurs contextes de sécurité, ou intercepter des données présentes dans un contexte normalement non accessible.

5 Solution

Se référer aux bulletins de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).
La version 10.63 corrige ces vulnérabilités.

6 Documentation

- Notes de mise à jour Windows Opera 10.63 :
<http://www.opera.com/docs/changelogs/windows/1063/>
- Notes de mise à jour Mac Opera 10.63 :
<http://www.opera.com/docs/changelogs/mac/1063/>
- Notes de mise à jour Unix Opera 10.63 :
<http://www.opera.com/docs/changelogs/unix/1063/>
- Téléchargement d'Opera :
<http://www.opera.com/download/browser/>
- Bulletins de sécurité Opera :
<http://www.opera.com/support/kb/view/971/>
<http://www.opera.com/support/kb/view/972/>
<http://www.opera.com/support/kb/view/973/>
<http://www.opera.com/support/kb/view/974/>
<http://www.opera.com/support/kb/view/976/>
- Référence CVE CVE-2010-4043 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4043>
- Référence CVE CVE-2010-4044 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4044>
- Référence CVE CVE-2010-4045 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4045>
- Référence CVE CVE-2010-4046 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4046>
- Référence CVE CVE-2010-4047 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4047>
- Référence CVE CVE-2010-4048 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4048>
- Référence CVE CVE-2010-4049 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4049>
- Référence CVE CVE-2010-4050 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4050>

Gestion détaillée du document

13 octobre 2010 version initiale.

27 octobre 2010 ajout des références CVE.