

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2005-AVI-367>

Gestion du document

Référence	CERTA-2005-AVI-367
Titre	Multiples vulnérabilités dans le navigateur Opera
Date de la première version	29 septembre 2005
Date de la dernière version	–
Source(s)	Bulletin de changement d'Opera
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 ;
- dépôt de fichiers arbitraires.

2 Systèmes affectés

Opera version 8.02 et versions antérieures

3 Description

Trois vulnérabilités ont été découvertes dans le navigateur Opera :

- La première permet le dépôt de fichiers arbitraires par l'exploitation d'une erreur dans la fonction de glisser/déposer.
- Les deux dernières permettent le contournement de la politique de sécurité par l'exploitation de deux autres erreurs présentes au niveau du traitement des cookies ou de la directive *must-revalidate*.

Ces vulnérabilités viennent se greffer aux deux vulnérabilités découvertes sur le client mail d'Opera, décrites dans l'avis CERTA-2005-AVI-355

4 Solution

La version 8.50 du navigateur Opera corrige ces vulnérabilités.

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

5 Documentation

- Site Internet du navigateur Opera :
<http://www.opera.com>
- Mise à jour Opéra :
<http://www.opera.com/docs/changelogs/windows/850>
<http://www.opera.com/docs/changelogs/linux/850>
- Références CVE :
 - CAN-2005-3059 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3059>
 - CAN-2005-3041 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3041>
- Référence CERTA-2005-AVI-355 : Vulnérabilités du client de messagerie d'Opera
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-355/CERTA-2005-AVI-355.html>
- Bulletin de sécurité SuSE et mise à jour :
<ftp://ftp.suse.com/pub/suse/>

Gestion détaillée du document

29 septembre 2005 version initiale.