Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S.G.D.S.N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 29 septembre 2005
N° CERTA-2005-AVI-355-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le client de messagerie d'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-355

Gestion du document

Référence	CERTA-2005-AVI-355-001
Titre	Vulnérabilités dans le client de messagerie d'Opera
Date de la première version	20 septembre 2005
Date de la dernière version	29 septembre 2005
Source(s)	Mise à jour de sécurité Opera version 8.02
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.

2 Systèmes affectés

Opera version 8.02 et versions antérieures.

3 Description

Deux vulnérabilités dans le client de messagerie d'Opera permettent, en les combinant, l'exécution de javascript malicieux.

- La première vulnérabilité permet de masquer l'extension réelle d'un fichier attaché en lui ajoutant le caractère point (".").
- La deuxième vulnérabilité permet l'ouverture non contrôlée des fichiers attachés, ce qui peut permettre l'exécution de javascript malicieux.

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-2005-3006 :
    http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3006
  - CAN-2005-3007 :
    http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3007
- Bulletin de sécurité suse et mise à jour :
  ftp://ftp.suse.com/pub/suse/

Gestion détaillée du document

20 septembre 2005 version initiale.
29 septembre 2005 ajout des références CVE, de la page de mise à jour Opera et de la mise à jour de Suse.