



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 août 2007
N° CERTA-2007-AVI-363-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2007-AVI-363>

Gestion du document

Référence	CERTA-2007-AVI-363-001
Titre	Vulnérabilités dans Opera
Date de la première version	16 août 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

- Exécution de code arbitraire à distance ;
- usurpation du contenu de la barre de navigation.

2 Systèmes affectés

Opera versions antérieures à 9.23.

3 Résumé

Deux vulnérabilités dans Opera permettent à une personne malintentionnée d'exécuter du code arbitraire à distance ou d'usurper le contenu de la barre de navigation de l'application.

4 Description

Une faille a été identifiée dans Opera, due à une erreur non spécifiée lors du traitement de code Javascript. Une personne peut ainsi exécuter du code arbitraire à distance sur le poste d'un utilisateur visitant une page web spécifiquement conçue.

Une seconde vulnérabilité dans Opera est causée par une erreur dans le traitement des URI (Universal Resource Identifier) de type data : . Elle permet à un utilisateur malintentionné d'usurper le contenu de la barre de navigation au moyen d'une URI spécialement construite.

5 Solution

La version 9.23 d'Opera corrige ce problème (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Opera :
<http://www.opera.com/support/search/view/865/>
- Mise à jour Opera 9.23 :
<http://www.opera.com/download/>
- Bulletin de sécurité Gentoo GLSA-200708-17 du 22 août 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200708-17.xml>
- Bulletin de sécurité SuSE SUSE-SR:2007:015 du 03 août 2007 :
<http://lists.opensuse.org/opensuse-security-announce/2007-08/msg00003.html>
- Référence CVE CVE-2007-3819 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3819>
- Référence CVE CVE-2007-4367 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4367>

Gestion détaillée du document

16 août 2007 version initiale.

27 août 2007 ajout d'une vulnérabilité, de la référence CVE et des bulletins de sécurité Gentoo et SuSE.