

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du navigateur et du client messagerie 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-2003-AVI-173>

Gestion du document

Référence	CERTA-2003-AVI-173-002
Titre	Vulnérabilité du navigateur et du client de messagerie Opera
Date de la première version	27 octobre 2003
Date de la dernière version	21 novembre 2003
Source(s)	Avis de sécurité Atstake a102003-1
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 versions 7.11 et 7.20.

3 Résumé

Une vulnérabilité dans le navigateur et le client de messagerie Opera permet à un utilisateur mal intentionné de faire exécuter par Opera du code arbitraire via une page HTML habilement construite.

4 Description

Opera est un navigateur et un client de messagerie disponible sur de nombreuses plates-formes. Le traitement du champ *HREF* dans une page HTML présente une vulnérabilité de type débordement de mémoire. Un utilisateur mal intentionné peut fabriquer une page HTML ou un courrier électronique avec un champ *HREF* contenant du code qui sera exécuté sur le système par l'intermédiaire du navigateur Opera.

5 Solution

Mettre à jour Opera en version 7.21. La nouvelle version est disponible sur le site d'Opera :
<http://www.opera.com/download/>

6 Documentation

- Avis de sécurité Atstake a102003-1 :
<http://www.atstake.com/research/advisories/2003/a102003-1.txt>
- Référence CVE CAN-2003-0870 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0870>
- Avis de sécurité Gentoo GLSA:200311-02 :
<http://www.securityfocus.com/archives/1/345062>

Gestion détaillée du document

27 octobre 2003 version initiale.

28 octobre 2003 première révision : correction de la référence CVE.

21 novembre 2003 seconde révision : ajout du bulletin de sécurité Gentoo.