



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 juillet 2004
N° CERTA-2004-AVI-231-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de plusieurs navigateurs

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-2004-AVI-231>

Gestion du document

Référence	CERTA-2004-AVI-231-002
Titre	Vulnérabilité de plusieurs navigateurs
Date de la première version	08 juillet 2004
Date de la dernière version	26 juillet 2004
Source(s)	Bulletin de sécurité Secunia SA11978 du 07 juillet 2004
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

- Usurpation du contenu de sites web ;
- récupération d'informations confidentielles.

2 Systèmes affectés

- Mozilla 0.x ;
- Mozilla versions 1.0 à 1.6 incluses ;
- Mozilla Firefox versions 0.x antérieures à la version 0.9 ;
- Opera versions 5.x, 6.x ;
- Opera versions 7.x antérieures à la version 7.52.

3 Résumé

Une vulnérabilité des navigateurs permet à un utilisateur mal intentionné d'usurper le contenu de sites web.

4 Description

Une vulnérabilité est présente dans plusieurs navigateurs dans la gestion des cadres (*frames*).

Lors de la visualisation d'un site web, si un lien doit ouvrir une URL dans un cadre particulier (désigné par l'instruction HTML *target*), le navigateur ne vérifie pas correctement si le cadre cible appartient à cette même fenêtre.

Il est possible pour un utilisateur mal intentionné, par le biais d'un lien HTML habilement construit, d'afficher une page web de son choix dans le cadre d'une fenêtre déjà ouverte du navigateur.

Cette vulnérabilité peut être exploitée pour usurper le contenu d'un site web, et recueillir ainsi des informations confidentielles (coordonnées personnelles ou bancaires, mots de passes, ...).

5 Contournement provisoire

Ne pas naviguer simultanément sur des sites de confiance et des sites non sûrs.

6 Solution

Mettre à jour le navigateur. Les versions suivantes corrigent cette vulnérabilité :

- Mozilla 1.7 ;
- Mozilla Firefox 0.9 et suivantes ;
- Opera 7.52.

7 Documentation

- Site Internet des navigateurs Mozilla et Firefox :
<http://www.mozilla.org>
- Site Internet du navigateur Opera :
<http://www.opera.com>
- Bulletin de sécurité Secunia SA11978 du 07 juillet 2004 :
<http://secunia.com/advisories/11978/>
- Bulletin de sécurité Gentoo pour Opera du 20 juillet 2004 :
<http://security.gentoo.org/glsa/glsa-200407-15.xml>
- Bulletin de sécurité OpenBSD pour Opera du 07 juillet 2004 :
<http://www.vuxml.org/openbsd/>
- Référence CVE CAN-2004-0717 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0717>
- Référence CVE CAN-2004-0718 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0718>

Gestion détaillée du document

08 juillet 2004 version initiale.

21 juillet 2004 ajout du bulletin de sécurité Gentoo.

26 juillet 2004 ajout références CVE.