



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 01 mars 2004  
N° CERTA-2004-AVI-052-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le navigateur Mozilla

---

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-052>

---

### Gestion du document

Référence	CERTA-2004-AVI-052-001
Titre	Vulnérabilité dans le navigateur Mozilla
Date de la première version	27 février 2004
Date de la dernière version	01 mars 2004
Source(s)	Avis de sécurité Mozilla
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

Attaque de type «Cross Site Scripting».

## 2 Systèmes affectés

- Mozilla 1.2;
- Mozilla 1.3;
- Mozilla 1.4;
- Mozilla 1.5;
- Mozilla 1.6.

## 3 Description

Mozilla est un navigateur «open source».

Une vulnérabilité découverte dans ce navigateur permet, lors du délai de passage d'une page web à une autre, d'interagir avec l'ancienne page. Un utilisateur mal intentionné peut déclencher par ce biais, par exemple, un programme javascript qui s'appliquera dans le domaine de la nouvelle page, et mener une attaque de type «cross-site scripting».

## **4 Solution**

Les dernières mises à jour de Mozilla (versions 1.4.2 et 1.6b) corrigent cette vulnérabilité.  
Ces versions peuvent être téléchargées sur le site de Mozilla :  
<http://www.mozilla.org>

## **5 Documentation**

Avis de sécurité de Mozilla :  
[http://bugzilla.mozilla.org/show\\_bug.cgi?id=227417](http://bugzilla.mozilla.org/show_bug.cgi?id=227417)  
Note d'information CERTA-2002-INF-001 : «Vulnérabilité de type « Cross Site Scripting »  
<http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-001/index.html>

## **Gestion détaillée du document**

**27 février 2004** version initiale ;

**01 mars 2004** correction typographique.