



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 mars 2008  
N° CERTA-2008-AVI-160-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Firefox

---

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-2008-AVI-160>

---

### Gestion du document

Référence	CERTA-2008-AVI-160-001
Titre	Vulnérabilités dans Firefox
Date de la première version	26 mars 2008
Date de la dernière version	27 mars 2008
Source(s)	Bulletin Mozilla du 25 mars 2008
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 ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

## 2 Systèmes affectés

*Firefox*, version 2.0.0.12 et antérieures.

## 3 Résumé

Plusieurs vulnérabilités affectent le navigateur *Firefox*. Leur exploitation permet à un utilisateur malveillant de contourner la politique de sécurité et en particulier d'exécuter du code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités affectent le navigateur *Firefox*.

Une erreur dans la gestion du protocole *jar* permet à un utilisateur malveillant d'ouvrir des connexions vers des ports arbitraires de la machine vulnérable.

Une erreur de gestion de certificats permet de divulguer des informations sensibles à un serveur malveillant.

Des erreurs dans le moteur d'affichage et dans l'interpréteur de *Javascript* permettent de provoquer des corruptions de mémoire. Ces corruptions sont exploitables pour exécuter indûment du code à distance.

Diverses erreurs permettent de :

- provoquer des injections de code indirectes (*cross-site scripting*) ;
- contourner des protections contre les attaques de type *cross-site request forgery* ;
- d'exécuter du code *Javascript* avec élévation de privilèges ;
- tromper l'utilisateur pour capturer ses identifiants et mots de passe.

## 5 Solution

La version 2.0.0.13 remédie à ces vulnérabilités.

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de la fondation Mozilla du 25 mars 2008 :  
<http://www.mozilla.org/projects/security/known-vulnerabilities.html#firefox2.0.0.13>
- Bulletin Red Hat RHSA-2008:0207-6 du 26 mars 2008 :  
<https://rhn.redhat.com/errata/RHSA-2008-0207.html>
- Bulletin Ubuntu USN-592-1 du 26 mars 2008 :  
<http://www.ubuntu.com/usn/usn-592-1>
- Référence CVE CVE-2007-4879 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4879>
- Référence CVE CVE-2008-1195 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1195>
- Référence CVE CVE-2008-1233 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1233>
- Référence CVE CVE-2008-1234 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1234>
- Référence CVE CVE-2008-1235 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1235>
- Référence CVE CVE-2008-1236 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1236>
- Référence CVE CVE-2008-1237 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1237>
- Référence CVE CVE-2008-1238 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1238>
- Référence CVE CVE-2008-1240 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1240>
- Référence CVE CVE-2008-1241 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1241>

## Gestion détaillée du document

**26 mars 2008** version initiale.

**27 mars 2008** ajout des bulletins de sécurité Ubuntu et Red Hat.