

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans les produits 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-2008-AVI-062>

---

### Gestion du document

Référence	CERTA-2008-AVI-062-001
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	08 février 2008
Date de la dernière version	11 février 2008
Source(s)	Annonce de la mise à jour Mozilla Firefox 2.0.0.12 du 07 février 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.

## 2 Systèmes affectés

- Mozilla Firefox pour les versions antérieures à 2.0.0.12 ;
- Mozilla SeaMonkey pour les versions antérieures 1.1.8 ;
- Mozilla Thunderbird pour les versions antérieures à 2.0.0.12.

A la date de rédaction de cet avis, la version 2.0.0.12 de Thunderbird n'est cependant pas téléchargeable sur le site officiel Mozilla.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le navigateur Mozilla Firefox. L'exploitation de ces dernières peut conduire notamment à l'exécution de code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités ont été identifiées dans le navigateur Mozilla Firefox. Parmi celles-ci :

- des vulnérabilités concernent le moteur JavaScript et provoquent sous certaines conditions une corruption de mémoire.
- le navigateur ne manipulerait pas correctement les contrôles d'entrée de fichiers associés à des balises de type `label`, pouvant provoquer le vol de fichiers arbitraires sur le poste de la victime ;
- des vulnérabilités permettent de contourner la politique de source commune (*same-origin policy*) et permettre d'injecter du code dans un autre site. L'une d'elle est rendue possible par la fonction `XMLDocument.load()` ;
- la gestion du stockage des mots de passe ne serait pas correcte : à l'ajout d'une entrée, le site distant pourrait altérer les mots de passe déjà présents et concernant d'autres sites ;
- l'URI `chrome:` permettrait de transgresser les droits d'accès et donc d'accéder à des fichiers (scripts ou images par exemple), lorsque certains modules complémentaires sont installés (CERTA-2008-ACT-004) ;
- les images ne sont pas correctement manipulées à la fermeture d'une page qui utilise des cadres `designMode`. Cette vulnérabilité permettrait ainsi de dérober des historiques de navigation ou perturber le navigateur.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Debian DSA-1484 du 10 février 2008 :  
<http://www.debian.org/security/2008/dsa-1484>
- Bulletin de sécurité Debian DSA-1485 du 10 février 2008 :  
<http://www.debian.org/security/2008/dsa-1485>
- Bulletin de sécurité Debian DSA-1489 du 10 février 2008 :  
<http://www.debian.org/security/2008/dsa-1489>
- Bulletin de sécurité RedHat RHSA-2008-0103 du 08 février 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0103.html>
- Bulletin de sécurité RedHat RHSA-2008-0104 du 08 février 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0104.html>
- Bulletin de sécurité RedHat RHSA-2008-0105 du 08 février 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0105.html>
- Bulletin de sécurité Ubuntu USN-576-1 du 08 février 2008 :  
<http://www.ubuntu.com/usn/usn-576-1>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-01 du 07 février 2008 :  
<http://www.mozilla.org/security/announce/2008/MFSA2008-01.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-02 du 07 février 2008 :  
<http://www.mozilla.org/security/announce/2008/MFSA2008-02.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-03 du 07 février 2008 :  
<http://www.mozilla.org/security/announce/2008/MFSA2008-03.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-04 du 07 février 2008 :  
<http://www.mozilla.org/security/announce/2008/MFSA2008-04.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-05 du 07 février 2008 :  
<http://www.mozilla.org/security/announce/2008/MFSA2008-05.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-06 du 07 février 2008 :  
<http://www.mozilla.org/security/announce/2008/MFSA2008-06.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-08 du 07 février 2008 :  
<http://www.mozilla.org/security/announce/2008/MFSA2008-08.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-09 du 07 février 2008 :  
<http://www.mozilla.org/security/announce/2008/MFSA2008-09.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-10 du 07 février 2008 :  
<http://www.mozilla.org/security/announce/2008/MFSA2008-10.html>

- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-11 du 07 février 2008 :  
<http://www.mozilla.org/security/announce/2008/MFSA2008-11.html>
- Référence CVE CVE-2008-0412 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0412>
- Référence CVE CVE-2008-0413 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0413>
- Référence CVE CVE-2008-0414 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0414>
- Référence CVE CVE-2008-0415 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0415>
- Référence CVE CVE-2008-0417 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0417>
- Référence CVE CVE-2008-0418 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0418>
- Référence CVE CVE-2008-0419 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0419>
- Référence CVE CVE-2008-0591 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0591>
- Référence CVE CVE-2008-0592 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0592>
- Référence CVE CVE-2008-0593 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0593>
- Référence CVE CVE-2008-0594 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0594>

## **Gestion détaillée du document**

**08 février 2008** version initiale.

**11 février 2008** ajout des références aux bulletins de sécurité Debian.