

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités des 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-473>

---

### Gestion du document

Référence	CERTA-2008-AVI-473-001
Titre	Multiples vulnérabilités des produits Mozilla
Date de la première version	24 septembre 2008
Date de la dernière version	14 octobre 2008
Source(s)	Bulletins de mise à jour Mozilla du 23 septembre 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 3.0.1 ;
- Mozilla Firefox 2.0.0.16 et versions antérieures ;
- Mozilla Thunderbird 2.0.0.16 et versions antérieures ;
- Mozilla SeaMonkey 1.1.11 et versions antérieures.

## 3 Résumé

De multiples vulnérabilités ont été découvertes dans les produits Mozilla. Ces vulnérabilités peuvent être exploitées afin réaliser des actions malveillantes diverses.

## 4 Description

Un très grand nombre de vulnérabilités ont été découvertes dans les produits Mozilla Firefox 3, Firefox 2, Thunderbird et SeaMonkey. L'exploitation de ces vulnérabilités permet à un utilisateur malintentionné de réaliser diverses actions, dont l'exécution de code arbitraire à distance.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Ubuntu  
<http://www.ubuntu.com/usn/usn-645-1>
- Bulletin de sécurité Ubuntu  
<http://www.ubuntu.com/usn/usn-645-2>
- Bulletin de sécurité Ubuntu  
<http://www.ubuntu.com/usn/usn-647-1>
- Bulletin de sécurité Redhat RHSA-2008-0879  
<http://rhn.redhat.com/erata/RHSA-2008-0879.html>
- Bulletin de sécurité FEDORA-2008-8399  
<https://www.redhat.com/archives/fedora-package-announce/2008-september/msg01362.html>
- Bulletin de sécurité FEDORA-2008-8425  
<https://www.redhat.com/archives/fedora-package-announce/2008-september/msg01334.html>
- Bulletin de sécurité FEDORA-2008-8425  
<https://www.redhat.com/archives/fedora-package-announce/2008-september/msg01335.html>
- Bulletin de sécurité FEDORA-2008-8401  
<https://www.redhat.com/archives/fedora-package-announce/2008-september/msg01384.html>
- Bulletin de sécurité FEDORA-2008-8429  
<https://www.redhat.com/archives/fedora-package-announce/2008-september/msg01403.html>
- Bulletin de sécurité Debian DSA-1649-1 du 08 octobre 2008 :  
<http://lists.debian.org/debian-security-announce/2008/msg00240.html>
- Bulletin de sécurité openSUSE SUSE-SA:2008:050 du 08 octobre 2008 :  
<http://lists.opensuse.org/opensuse-security-announce/2008-10/msg00005.html>
- Bulletin de sécurité RedHat RHSA-2008:0882-24 du 23 septembre 2008 :  
<http://rhn.redhat.com/errata/RHSA-2008-0882/html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-37 du 23 septembre 2008 :  
<http://www.mozilla.org/security/announce/2008/mfsa2008-37.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-38 du 23 septembre 2008 :  
<http://www.mozilla.org/security/announce/2008/mfsa2008-38.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-39 du 23 septembre 2008 :  
<http://www.mozilla.org/security/announce/2008/mfsa2008-39.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-40 du 23 septembre 2008 :  
<http://www.mozilla.org/security/announce/2008/mfsa2008-40.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-41 du 23 septembre 2008 :  
<http://www.mozilla.org/security/announce/2008/mfsa2008-41.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-42 du 23 septembre 2008 :  
<http://www.mozilla.org/security/announce/2008/mfsa2008-42.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-43 du 23 septembre 2008 :  
<http://www.mozilla.org/security/announce/2008/mfsa2008-43.html>
- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-44 du 23 septembre 2008 :  
<http://www.mozilla.org/security/announce/2008/mfsa2008-44.html>

- Bulletin de sécurité de la fondation Mozilla 2008/MFSA2008-45 du 23 septembre 2008 :  
<http://www.mozilla.org/security/announce/2008/mfsa2008-45.html>
- Référence CVE CVE-2008-0016 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0016>
- Référence CVE CVE-2008-3835 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3835>
- Référence CVE CVE-2008-3837 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3837>
- Référence CVE CVE-2008-4058 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4058>
- Référence CVE CVE-2008-4059 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4059>
- Référence CVE CVE-2008-4060 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4060>
- Référence CVE CVE-2008-4061 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4061>
- Référence CVE CVE-2008-4062 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4062>
- Référence CVE CVE-2008-4065 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4065>
- Référence CVE CVE-2008-4066 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4066>
- Référence CVE CVE-2008-4067 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4067>
- Référence CVE CVE-2008-4068 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4068>
- Référence CVE CVE-2008-4069 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4069>

## **Gestion détaillée du document**

**24 septembre 2008** version initiale.

**30 septembre 2008** Ajout Ubuntu et FEDORA

**14 octobre 2008** Ajout des références aux bulletins de sécurité Debian, openSUSE et RedHat.