

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-2011-AVI-267>

---

### Gestion du document

Référence	CERTA-2011-AVI-267-002
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	29 avril 2011
Date de la dernière version	05 mai 2011
Source(s)	Bulletins de sécurité de la fondation Mozilla mfsa2011-12 à mfsa2011-18 du 28 avril 2011
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.

## 2 Systèmes affectés

Les versions antérieures aux versions suivantes :

- Firefox 4.0.1 ;
- Firefox 3.6.17 ;
- Firefox 3.5.19 ;
- Thunderbird 3.1.10 ;
- SeaMonkey 2.0.14.

## 3 Résumé

De multiples vulnérabilités ont été corrigées dans les produits Mozilla, dont certaines permettent l'exécution de code arbitraire à distance.

## 4 Description

De multiples vulnérabilités ont été corrigées dans les produits Mozilla :

- plusieurs vulnérabilités dans la gestion de la mémoire par le moteur de navigation utilisé dans Firefox, Thunderbird et Seamonkey peuvent être exploitées pour corrompre la mémoire et exécuter du code arbitraire à distance ;
- plusieurs vulnérabilités dans la fonction WebGL et les bibliothèques WebGLES introduites avec Firefox 4.0 permettent d'exécuter du code arbitraire et de contourner certaines protections des versions récentes de Microsoft Windows comme l'ASLR ;
- une vulnérabilité dans la fonction XSLT generate-id() révèle l'adresse mémoire d'un objet du tas et peut être utilisée pour renforcer une attaque exploitant d'autres vulnérabilités.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-12 du 28 avril 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-12.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-13 du 28 avril 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-13.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-14 du 28 avril 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-14.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-15 du 28 avril 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-15.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-16 du 28 avril 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-16.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-17 du 28 avril 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-17.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-18 du 28 avril 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-18.html>
- Bulletin de sécurité Debian DSA-2227 du 30 avril 2011 :  
<http://www.debian.org/security/2011/dsa-2227>
- Bulletin de sécurité Debian DSA-2228 du 01 mai 2011 :  
<http://www.debian.org/security/2011/dsa-2228>
- Bulletin de sécurité Ubuntu USN-1112 du 29 avril 2011 :  
<http://www.ubuntu.com/usn/usn-1112-1/>
- Bulletin de sécurité Ubuntu USN-1122 du 05 mai 2011 :  
<http://www.ubuntu.com/usn/usn-1122-1/>
- Bulletin de sécurité Fedora FEDORA-2011-6215 du 29 avril 2011 :  
<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/059185.html>
- Bulletin de sécurité Fedora FEDORA-2011-6215 du 29 avril 2011 :  
<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/059187.html>
- Bulletin de sécurité Fedora FEDORA-2011-6215 du 29 avril 2011 :  
<http://lists.fedoraproject.org/pipermail/package-announce/2011-April/059189.html>
- Référence CVE CVE-2011-0065 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0065>
- Référence CVE CVE-2011-0066 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0066>
- Référence CVE CVE-2011-0067 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0067>
- Référence CVE CVE-2011-0068 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0068>

- Référence CVE CVE-2011-0069 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0069>
- Référence CVE CVE-2011-0070 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0070>
- Référence CVE CVE-2011-0071 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0071>
- Référence CVE CVE-2011-0072 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0072>
- Référence CVE CVE-2011-0073 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0073>
- Référence CVE CVE-2011-0074 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0074>
- Référence CVE CVE-2011-0075 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0075>
- Référence CVE CVE-2011-0076 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0076>
- Référence CVE CVE-2011-0077 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0077>
- Référence CVE CVE-2011-0078 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0078>
- Référence CVE CVE-2011-0079 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0079>
- Référence CVE CVE-2011-0080 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0080>
- Référence CVE CVE-2011-0081 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0081>
- Référence CVE CVE-2011-1202 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1202>

## **Gestion détaillée du document**

**29 avril 2011** version initiale.

**04 mai 2011** ajout des bulletins de sécurité Debian, Fedora et Ubuntu.

**05 mai 2011** ajout du bulletins de sécurité Ubuntu pour Thunderbird.