



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 29 septembre 2011  
N° CERTA-2011-AVI-537

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-537>

---

### Gestion du document

Référence	CERTA-2011-AVI-537
Titre	Multiples vulnérabilités dans les produits Mozilla
Date de la première version	29 septembre 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité de la fondation Mozilla du 27 septembre 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 ;
- déni de service à distance ;
- élévation de privilèges.

## 2 Systèmes affectés

- Firefox versions antérieures à 7.0 ;
- Firefox versions antérieures à 3.6.23 ;
- Thunderbird versions antérieures à 7.0 ;
- SeaMonkey versions antérieures à 2.4.

## 3 Résumé

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

## 4 Description

Plusieurs vulnérabilités ont été corrigées dans les produits de la fondation Mozilla, en particulier :

- des problèmes de corruption mémoire qui pourraient autoriser l'exécution de code arbitraire à distance ;
- une erreur de type débordement d'entier dans une expression javascript ;
- une erreur dans la gestion des cadres permettrait le contournement du cloisonnement des pages dans les plugins ;
- l'installation de code malveillant en incitant l'utilisateur à maintenir enfoncée la touche 'Entrée' ;
- une erreur de type dépassement de tampon dans WebGL ;
- un arrêt inopiné potentiellement exploitable dans une bibliothèque javascript ;
- une vulnérabilité dans la fonction JSSubScript utilisée par certains modules pouvant être exploitée par du contenu web malveillant pour élever ses privilèges ;
- l'exécution de code arbitraire à l'aide d'un fichier .ogg spécialement conçu.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité de la fondation Mozilla /mfsa2011-36 du 27 septembre 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-36.html>
- Bulletin de sécurité de la fondation Mozilla /mfsa2011-37 du 27 septembre 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-37.html>
- Bulletin de sécurité de la fondation Mozilla /mfsa2011-38 du 27 septembre 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-38.html>
- Bulletin de sécurité de la fondation Mozilla /mfsa2011-39 du 27 septembre 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-39.html>
- Bulletin de sécurité de la fondation Mozilla /mfsa2011-40 du 27 septembre 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-40.html>
- Bulletin de sécurité de la fondation Mozilla /mfsa2011-41 du 27 septembre 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-41.html>
- Bulletin de sécurité de la fondation Mozilla /mfsa2011-42 du 27 septembre 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-42.html>
- Bulletin de sécurité de la fondation Mozilla /mfsa2011-43 du 27 septembre 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-43.html>
- Bulletin de sécurité de la fondation Mozilla /mfsa2011-44 du 27 septembre 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-44.html>
- Bulletin de sécurité de la fondation Mozilla /mfsa2011-45 du 27 septembre 2011 :  
<http://www.mozilla.org/security/announce/2011/mfsa2011-45.html>
- Référence CVE CVE-2011-2372 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2372>
- Référence CVE CVE-2011-2995 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2995>
- Référence CVE CVE-2011-2999 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2999>
- Référence CVE CVE-2011-3000 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3000>
- Référence CVE CVE-2011-3001 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3001>
- Référence CVE CVE-2011-3002 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3002>

- Référence CVE CVE-2011-3003 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3003>
- Référence CVE CVE-2011-3004 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3004>
- Référence CVE CVE-2011-3005 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3005>
- Référence CVE CVE-2011-3232 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3232>

## **Gestion détaillée du document**

**29 septembre 2011** version initiale.