

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : 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-712>

---

### Gestion du document

Référence	CERTA-2011-AVI-712
Titre	Vulnérabilités dans les produits Mozilla
Date de la première version	21 décembre 2011
Date de la dernière version	–
Source(s)	Bulletins de sécurité Mozilla MFSA2011-53 à MFSA2011-59 du 20 décembre 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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Mozilla Firefox versions antérieures à la version 9.0 ;
- Mozilla Firefox 3.x : versions antérieures à la version 3.6.25 ;
- Mozilla Thunderbird versions antérieures à la version 9.0 ;
- Mozilla Thunderbird 3.x : versions antérieures à la version 3.1.17 ;
- Mozilla SeaMonkey versions antérieures à la version 2.6 ;

## 3 Résumé

Plusieurs vulnérabilités ont été corrigées dans les produits Mozilla dont certaines permettent à un utilisateur malintentionné d'exécuter du code arbitraire à distance.

## 4 Description

Plusieurs vulnérabilités ont été corrigées dans les produits Mozilla :

- mfsa2011-53 : plusieurs problèmes de gestion mémoire peuvent être exploités dans le but d'exécuter du code arbitraire à distance ;
- mfsa2011-54 : un arrêt inopiné de l'application peut être provoqué à partir de certaines expressions régulières spécialement conçues et utilisées dans du javascript ;
- mfsa2011-55 : une erreur dans la gestions d'éléments SVG permet, sous certaines conditions, un accès à une zone non autorisée de la mémoire ;
- mfsa2011-56 : une erreur dans la gestion d'éléments SVG permet à un site malveillant d'enregistrer des frappes clavier de l'utilisateur ;
- mfsa2011-57 : une exécution de code arbitraire à distance ou un arrêt inopiné de l'application peut être provoqué par un greffon (*plugin*) spécialement conçu (Mac OS X uniquement) ;
- mfsa2011-58 : un arrêt inopiné de l'application peut être provoqué en utilisant un élément *OGG* spécialement conçu ;
- mfsa2011-59 : une installation de code malveillant peut être provoqué en incitant l'utilisateur à maintenir enfoncée la touche « Entrée » (Mac OS X uniquement).

## 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/mfsa2011-53 du 20 décembre 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-53.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-54 du 20 décembre 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-54.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-55 du 20 décembre 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-55.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-56 du 20 décembre 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-56.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-57 du 20 décembre 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-57.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-58 du 20 décembre 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-58.html>
- Bulletin de sécurité de la fondation Mozilla 2011/mfsa2011-59 du 20 décembre 2011 : <http://www.mozilla.org/security/announce/2011/mfsa2011-59.html>
- Référence CVE CVE-2011-3658 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3658>
- Référence CVE CVE-2011-3660 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3660>
- Référence CVE CVE-2011-3661 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3661>
- Référence CVE CVE-2011-3663 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3663>
- Référence CVE CVE-2011-3664 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3664>
- Référence CVE CVE-2011-3665 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3665>
- Référence CVE CVE-2011-3666 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3666>

# **Gestion détaillée du document**

**21 décembre 2011** version initiale.