

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Vulnérabilité dans Mozilla Firefox

---

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-2009-ALE-012>

---

### Gestion du document

Référence	CERTA-2009-ALE-012-001
Titre	Vulnérabilité dans Mozilla Firefox
Date de la première version	15 juillet 2009
Date de la dernière version	17 juillet 2009
Source(s)	Bulletin de sécurité Secunia 35798 du 14 juillet 2009
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

Mozilla Firefox 3.5.

## 3 Résumé

Une vulnérabilité affectant le traitement d'une balise HTML permet à une personne malveillante d'exécuter du code arbitraire à distance.

## 4 Description

Une vulnérabilité affectant le traitement de la balise `<font>` par l'interpréteur JavaScript permet à une personne malveillante d'exécuter du code arbitraire à distance au moyen d'une page web spécialement écrite.

Un code permettant l'exploitation de cette vulnérabilité est disponible sur l'Internet.

## 5 Contournement provisoire

Dans l'attente d'un correctif le CERTA recommande d'utiliser un navigateur alternatif ou de naviguer avec le JavaScript désactivé.

## 6 Solution

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

## 7 Documentation

- Bulletin de sécurité de la fondation Mozilla MFSA 2009-41 du 16 juillet 2009 :  
<http://www.mozilla.org/security/announce/2009/mfsa2009-41.html>
- Bulletin de sécurité Secunia 35798 du 14 juillet 2009 :  
<http://secunia.com/advisories/35798>
- Article de sécurité Mozilla du 14 juillet :  
<http://blog.mozilla.com/security/2009/07/14/critical-javascript-vulnerability-in-firefox-35/>
- Référence NIST du CVE-2009-2477 :  
<http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2477>
- Référence CVE CVE-2009-2477 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2477>

## Gestion détaillée du document

**15 juillet 2009** version initiale.

**17 juillet** ajout des liens Mozilla et CVE.