

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-AVI-290>

---

### Gestion du document

Référence	CERTA-2009-AVI-290
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	24 juillet 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité MFSA2009-34 à MFSA2009-40 du 21 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 ;
- injection de code indirecte.

## 2 Systèmes affectés

Mozilla Firefox versions antérieures à la 3.5.1.

## 3 Résumé

De multiples vulnérabilités ont été découvertes dans Mozilla Firefox et permettent à une personne mal-intentionnée distante d'effectuer des injections de code indirectes et d'exécuter du code arbitraire.

## 4 Description

Plusieurs vulnérabilités dans Mozilla Firefox ont été découvertes :

- plusieurs erreurs dans la gestion de la mémoire ont été corrigées ;

- une erreur dans l'intégration du module *Flash* permet une exécution de code arbitraire à distance ;
- une erreur dans la gestion de certaines polices de caractères permet à une personne distante malveillante d'exécuter du code arbitraire ;
- un problème relatif aux éléments *SVG (Scalable Vector Graphics)* peut conduire à une exécution de code arbitraire à distance ;
- une exécution de code arbitraire est possible via la fonction *setTimeout()* dans certaines conditions ;
- des injections de code indirectes peuvent être menées par l'intermédiaire de certains objets.

## 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 MFSA2009-34 du 21 juillet 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-34.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-35 du 21 juillet 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-35.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-36 du 21 juillet 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-36.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-37 du 21 juillet 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-37.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-38 du 21 juillet 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-38.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-39 du 21 juillet 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-39.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-40 du 21 juillet 2009 : <http://www.mozilla.org/security/announce/2009/mfsa2009-40.html>
- Référence CVE CVE-2009-1194 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1194>
- Référence CVE CVE-2009-2462 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2462>
- Référence CVE CVE-2009-2463 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2463>
- Référence CVE CVE-2009-2464 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2464>
- Référence CVE CVE-2009-2465 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2465>
- Référence CVE CVE-2009-2466 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2466>
- Référence CVE CVE-2009-2467 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2467>
- Référence CVE CVE-2009-2468 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2468>
- Référence CVE CVE-2009-2469 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2469>
- Référence CVE CVE-2009-2471 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2471>
- Référence CVE CVE-2009-2472 : <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2472>

## Gestion détaillée du document

24 juillet 2009 version initiale.