

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-459>

---

### Gestion du document

Référence	CERTA-2009-AVI-459-001
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	28 octobre 2009
Date de la dernière version	04 novembre 2009
Source(s)	Bulletins de sécurité de la fondation Mozilla du 27 octobre 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

*Mozilla Firefox*, versions 3.0.x et 3.5.x.

## 3 Résumé

De nombreuses vulnérabilités de *Mozilla Firefox* ont été publiées. Certaines permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

## 4 Description

De nombreuses vulnérabilités de *Mozilla Firefox* ont été publiées :

- une erreur de traitement du formulaire d'historique permet de lire des informations sans en avoir le droit ;
- la prévisibilité des noms des fichiers téléchargés est exploitable par un utilisateur malveillant ayant un accès au système vulnérable pour exécuter du code arbitraire ;
- une mauvaise gestion de récursivité permet à un utilisateur malveillant de provoquer un déni de service, voire exécuter du code arbitraire ;
- un traitement défectueux des fichiers de configuration automatique (PAC) permet à un utilisateur malveillant de provoquer un déni de service à distance, voire exécuter du code arbitraire, quand le navigateur est configuré pour utiliser ces fichiers ;
- une mauvaise analyse des images au format GIF permet à un utilisateur malveillant de provoquer un déni de service à distance, voire exécuter du code arbitraire ;
- le module XPCOM comporte un défaut exploitable pour exécuter des JavaScripts avec des privilèges élevés ;
- la conversion des chaînes de caractères en nombres en virgule flottante comporte un défaut exploitable pour exécuter du code arbitraire ;
- la fonction JavaScript `document.getSelection` ne respecte pas la politique de séparation des domaines ;
- le caractère unicode d'inversion du sens de lecture (*Right to left override character*) inclus dans un nom de fichier peut tromper l'utilisateur sur la nature de l'objet qu'il télécharge.

## 5 Solution

Les versions 3.0.15 et 3.5.4 remédient à ces problèmes.

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

## 6 Documentation

- Bulletins de sécurité de la fondation Mozilla 2009/mfsa2009-52 et suivants du 27 octobre 2009 :
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-52.html>
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-53.html>
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-54.html>
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-55.html>
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-56.html>
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-57.html>
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-59.html>
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-61.html>
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-62.html>
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-63.html>
  - <http://www.mozilla.org/security/announce/2009/mfsa2009-64.html>
- Bulletin de sécurité Debian DSA-1922 du 28 octobre 2009 :
  - <http://www.debian.org/security/2009/dsa-1922>
- Bulletin de sécurité RedHat RHSA-2009:1530 du 27 octobre 2009 :
  - <http://rhn.redhat.com/errata/RHSA-2009-1530.html>
- Bulletin de sécurité RedHat RHSA-2009:1531 du 27 octobre 2009 :
  - <http://rhn.redhat.com/errata/RHSA-2009-1531.html>
- Bulletin de sécurité Ubuntu USN-853-1 du 31 octobre 2009 :
  - <http://www.ubuntu.com/usn/USN-853-1>
- Référence CVE CVE-2009-1563 :
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1563>
- Référence CVE CVE-2009-3370 :
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3370>
- Référence CVE CVE-2009-3371 :
  - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3371>

- Référence CVE CVE-2009-3372 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3372>
- Référence CVE CVE-2009-3373 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3373>
- Référence CVE CVE-2009-3374 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3374>
- Référence CVE CVE-2009-3375 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3375>
- Référence CVE CVE-2009-3376 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3376>
- Référence CVE CVE-2009-3377 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3377>
- Référence CVE CVE-2009-3378 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3378>
- Référence CVE CVE-2009-3379 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3379>
- Référence CVE CVE-2009-3380 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3380>
- Référence CVE CVE-2009-3381 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3381>
- Référence CVE CVE-2009-3382 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3382>
- Référence CVE CVE-2009-3383 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3383>

## **Gestion détaillée du document**

**28 octobre 2009** version initiale.

**04 novembre 2009** ajout des références aux bulletins de sécurité Debian, RedHat et Ubuntu.