



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 16 décembre 2009  
N° CERTA-2009-AVI-547

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-547>

---

### Gestion du document

Référence	CERTA-2009-AVI-547
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	16 décembre 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité de la fondation Mozilla du 15 décembre 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.

## 2 Systèmes affectés

- *Firefox* versions 3.5.x antérieures à 3.5.6 ;
- *Firefox* versions 3.0.x antérieures à 3.0.16 ;
- *Seamonkey* versions antérieures à 2.0.1.

## 3 Résumé

De multiples vulnérabilités dans *Firefox* permettent l'exécution de code arbitraire à distance.

## 4 Description

De multiples vulnérabilités ont été découvertes dans *Firefox* :

- plusieurs problèmes de stabilité affectent le moteur du navigateur. Certains mènent à une corruption de la mémoire et permettent l'exécution de code arbitraire à distance ;
- des failles dans `liboggplay` permettent l'exécution de code arbitraire à distance ;
- une vulnérabilité de type débordement d'entier dans `libtheora` permet l'exécution de code arbitraire à distance. Un autre problème dans cette bibliothèque peut être exploité pour provoquer un déni de service à distance ;
- l'implémentation *Mozilla* de NTLM permet de rejouer les identifiants de connexion d'une application à une autre via le navigateur ;
- un problème dans la gestion des codes retour 204 peut leurrer un utilisateur en lui donnant l'illusion qu'il est sur une page sécurisée alors que ce n'est pas le cas. Une vulnérabilité similaire permet d'injecter du code dans une page vide ;
- du code `Javascript` peut être exécuté par l'intermédiaire de la fenêtre `chrome` ;
- les messages d'exception engendrés par `GeckoActiveXObject` varient en fonction des identifiants `ProgID` d'objets `COM` présents dans le registre du système. Un site malveillant peut obtenir la liste des objets `COM` installés sur le système de l'internaute.

## 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 2009/mfsa2009-65 du 15 décembre 2009 :  
<http://www.mozilla.org/security/announce/2009/mfsa2009-65.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-66 du 15 décembre 2009 :  
<http://www.mozilla.org/security/announce/2009/mfsa2009-66.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-67 du 15 décembre 2009 :  
<http://www.mozilla.org/security/announce/2009/mfsa2009-67.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-68 du 15 décembre 2009 :  
<http://www.mozilla.org/security/announce/2009/mfsa2009-68.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-69 du 15 décembre 2009 :  
<http://www.mozilla.org/security/announce/2009/mfsa2009-69.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-70 du 15 décembre 2009 :  
<http://www.mozilla.org/security/announce/2009/mfsa2009-70.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-71 du 15 décembre 2009 :  
<http://www.mozilla.org/security/announce/2009/mfsa2009-71.html>
- Référence CVE CVE-2009-3388 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3388>
- Référence CVE CVE-2009-3389 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3389>
- Référence CVE CVE-2009-3979 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3979>
- Référence CVE CVE-2009-3980 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3980>
- Référence CVE CVE-2009-3981 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3981>
- Référence CVE CVE-2009-3982 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3982>
- Référence CVE CVE-2009-3983 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3983>

- Référence CVE CVE-2009-3984 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3984>
- Référence CVE CVE-2009-3985 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3985>
- Référence CVE CVE-2009-3986 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3986>
- Référence CVE CVE-2009-3987 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3987>

## **Gestion détaillée du document**

**16 décembre 2009** version initiale.