Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 avril 2009
N° CERTA-2009-AVI-157

**Affaire suivie par :**
CERTA

# AVIS DU CERTA

## Objet : Multiples vulnérabilités dans Mozilla Firefox



## Gestion du document

| | |
|---|---|
| Référence | CERTA-2009-AVI-157 |
| Titre | Multiples vulnérabilités dans Mozilla Firefox |
| Date de la première version | 22 avril 2009 |
| Date de la dernière version | – |
| Source(s) | Notes de mise à jour Mozilla Firefox 3.0.9 du 21 avril 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 ;
- injection de requêtes illégitimes par rebond.

## 2 Systèmes affectés

- Les versions de Mozilla Firefox antérieures à 3.0.9.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le navigateur Mozilla Firefox. L'exploitation de celles-ci peut avoir des conséquences variées, du contournement de la politique de sécurité mise en place à l'exécutation de code arbitraire au cours d'une navigation sur une page spécialement construite.

# 4 Description

Plusieurs vulnérabilités ont été identifiées dans le navigateur Mozilla Firefox. Parmi celles-ci :

– le moteur de navigation Mozilla manipule incorrectement certaines pages Web lorsque l'interprétation de code Javascript est active. Cela provoque une corruption de la mémoire pouvant conduire, sous certaines conditions, à l'exécution de code arbitraire à distance ;
– l'interprétation de certains caractères graphiques est prise en compte par l'IDN (*International Domain Names*) et peut ainsi être détournée pour favoriser des attaques en filoutage (*phishing*) ;
– le module Flash confond l'origine du contenu sous certaines conditions, ce qui permet alors au code interprété d'accéder illégitimement à certaines ressources (accès arbitraires en lecture et écriture des *Local Shared Objects* par exemple) ;
– le navigateur ne manipule pas correctement les données de rafraichissement dans les en-têtes (*Refresh*) permettant à une page malveillante de lancer des attaques par injection de code indirecte ou à forcer, sous certaines conditions, le navigateur à interpréter du code JavaScript arbitraire dans le contexte d'un site victime.

# 5 Solution

Se référer aux avis de sécurité de Mozilla pour l'obtention des correctifs (cf. section Documentation).

# 6 Documentation

– Notes de mise à jour Mozilla Firefox 3.0.9 du 21 avril 2009 :
http://www.mozilla.com/en-US/firefox/3.0.9/releasenotes/
– Avis de sécurité Mozilla pour Firefox 3.0 :
http://www.mozilla.org/security/known-vulnerabilities/firefox30.html#firefox3.0.9
– Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-14 du 21 avril 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-14.html
– Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-15 du 21 avril 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-15.html
– Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-16 du 21 avril 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-16.html
– Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-17 du 21 avril 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-17.html
– Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-18 du 21 avril 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-18.html
– Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-19 du 21 avril 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-19.html
– Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-20 du 21 avril 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-20.html
– Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-21 du 21 avril 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-21.html
– Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-22 du 21 avril 2009 :
http://www.mozilla.org/security/announce/2009/mfsa2009-22.html
– Référence CVE CVE-2009-0652 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0652
– Référence CVE CVE-2009-1302 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1302
– Référence CVE CVE-2009-1303 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1303
– Référence CVE CVE-2009-1304 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1304
– Référence CVE CVE-2009-1305 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1305

- Référence CVE CVE-2009-1306 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1306
- Référence CVE CVE-2009-1307 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1307
- Référence CVE CVE-2009-1308 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1308
- Référence CVE CVE-2009-1309 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1309
- Référence CVE CVE-2009-1310 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1310
- Référence CVE CVE-2009-1311 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1311
- Référence CVE CVE-2009-1312 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1312

## Gestion détaillée du document

**22 avril 2009** version initiale.