Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 01 avril 2010
N° CERTA-2010-AVI-149

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Firefox

Gestion du document

Référence	CERTA-2010-AVI-149
Titre	Multiples vulnérabilités dans Firefox
Date de la première version	01 avril 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité de la fondation Mozilla 2010/mfsa2010-16 à 24 du 30 mars 2010
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 3.6.x, 3.5.x, 3.0.x.

3 Résumé

De multiples vulnérabilités affectent Firefox dont les plus importantes permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance sur le système vulnérable.

4 Description

Plusieurs vulnérabilités affectent Firefox :

- dans certaines circonstances, le navigateur s'arrête de manière inopinée, permettant à un attaquant de provoquer un déni de service à distance ;
- plusieurs défauts dans l'allocation de la mémoire et dans la gestion des pointeurs permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance ;
- la possibilité pour une applette de détourner des clics de souris permet à un utilisateur malveillant d'exécuter du code arbitraire à distance ;
- un défaut dans l'extension Firebug permet à un utilisateur malveillant d'exécuter du code arbitraire à distance ;
- un défaut dans le traitement du protocole SSL permet à un utilisateur distant de contourner la politique de sécurité ;
- la présence d'un lien `mailto:` dans un objet image provoque le lancement du client de messagerie. L'impact est un désagrément ;
- des vérifications omises pendant le traitement de documents XML peuvent conduire au chargement d'objets non permis par la politique de sécurité.

5 Solution

Les versions Firefox 3.6.2 et 3.5.9 remédient à toutes les vulnérabilités.

La version 3.0.19 remédie aux vulnérabités sauf les deux dernières. La branche 3.0 n'étant désormais plus maintenue, la migration vers les branches 3.5 ou 3.6 offre une solution de plus long terme.

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 2010/mfsa2010-16 du 30 mars 2010 : http://www.mozilla.org/security/announce/2010/mfsa2010-16.html
- Bulletin de sécurité de la fondation Mozilla 2010/mfsa2010-17 du 30 mars 2010 : http://www.mozilla.org/security/announce/2010/mfsa2010-17.html
- Bulletin de sécurité de la fondation Mozilla 2010/mfsa2010-18 du 30 mars 2010 : http://www.mozilla.org/security/announce/2010/mfsa2010-18.html
- Bulletin de sécurité de la fondation Mozilla 2010/mfsa2010-19 du 30 mars 2010 : http://www.mozilla.org/security/announce/2010/mfsa2010-19.html
- Bulletin de sécurité de la fondation Mozilla 2010/mfsa2010-20 du 30 mars 2010 : http://www.mozilla.org/security/announce/2010/mfsa2010-20.html
- Bulletin de sécurité de la fondation Mozilla 2010/mfsa2010-21 du 30 mars 2010 : http://www.mozilla.org/security/announce/2010/mfsa2010-21.html
- Bulletin de sécurité de la fondation Mozilla 2010/mfsa2010-22 du 30 mars 2010 : http://www.mozilla.org/security/announce/2010/mfsa2010-22.html
- Bulletin de sécurité de la fondation Mozilla 2010/mfsa2010-23 du 30 mars 2010 : http://www.mozilla.org/security/announce/2010/mfsa2010-23.html
- Bulletin de sécurité de la fondation Mozilla 2010/mfsa2010-24 du 30 mars 2010 : http://www.mozilla.org/security/announce/2010/mfsa2010-24.html
- Référence CVE CVE-2009-3555 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555
- Référence CVE CVE-2010-0173 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0173
- Référence CVE CVE-2010-0174 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0174
- Référence CVE CVE-2010-0175 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0175

- Référence CVE CVE-2010-0176 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0176
- Référence CVE CVE-2010-0177 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0177
- Référence CVE CVE-2010-0178 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0178
- Référence CVE CVE-2010-0179 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0179
- Référence CVE CVE-2010-0181 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0181
- Référence CVE CVE-2010-0182 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0182

Gestion détaillée du document

01 avril 2010 version initiale.