

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-233>

Gestion du document

Référence	CERTA-2009-AVI-233
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	12 juin 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Mozilla MFSA 2009-24 à 2009-32 du 11 juin 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, toutes versions antérieures à la 3.0.11.

3 Résumé

De multiples vulnérabilités dans Mozilla Firefox permettent, entre autres, à une personne malveillante d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités dans Mozilla Firefox ont été découvertes :

- plusieurs vulnérabilités dans le moteur du navigateur permettent une exécution de code arbitraire à distance (CVE-2009-1392, CVE-2009-1832 et CVE-2009-1833) ;
- une erreur dans l'interprétation de certains caractères *unicode* permet à une personne malveillante d'afficher une *URL* trompeuse (CVE-2009-1834) ;
- une ressource locale exécutée via le protocole *file*: permet d'accéder aux fichiers de session de l'utilisateur (CVE-2009-1835) ;
- une erreur dans la gestion des réponses différentes du code « 200 » après une requête *CONNECT* à un serveur mandataire permet à une personne malveillante d'exécuter du code arbitraire (CVE-2009-1836) ;
- une erreur dans la gestion des objets *Java* permet à une personne distante d'exécuter du code arbitraire (CVE-2009-1837) ;
- une erreur dans l'interpréteur d'événements permet d'exécuter du code *JavaScript* avec les privilèges *chrome* (CVE-2009-1838) ;
- une erreur dans la gestion des permissions via le protocole *file*: permet à un nouveau document chargé d'obtenir des droits du document précédemment ouvert (CVE-2009-1839) ;
- une vulnérabilité existe dans le contrôle des politiques de chargement de contenu avant l'exécution de scripts externes d'un fichier *XUL* (CVE-2009-1840) ;
- une erreur lorsqu'un objet avec les droits *chrome* interagit avec du contenu web permet à une personne malintentionnée d'exécuter du code arbitraire.

5 Solution

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

6 Documentation

- Bulletin de sécurité de la fondation Mozilla mfsa2009-24 du 11 juin 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-24.html>
- Bulletin de sécurité de la fondation Mozilla mfsa2009-25 du 11 juin 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-25.html>
- Bulletin de sécurité de la fondation Mozilla mfsa2009-26 du 11 juin 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-26.html>
- Bulletin de sécurité de la fondation Mozilla mfsa2009-27 du 11 juin 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-27.html>
- Bulletin de sécurité de la fondation Mozilla mfsa2009-28 du 11 juin 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-28.html>
- Bulletin de sécurité de la fondation Mozilla mfsa2009-29 du 11 juin 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-29.html>
- Bulletin de sécurité de la fondation Mozilla mfsa2009-30 du 11 juin 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-30.html>
- Bulletin de sécurité de la fondation Mozilla mfsa2009-31 du 11 juin 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-31.html>
- Bulletin de sécurité de la fondation Mozilla mfsa2009-32 du 11 juin 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-32.html>
- Référence CVE CVE-2009-1392 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1392>
- Référence CVE CVE-2009-1832 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1832>
- Référence CVE CVE-2009-1833 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1833>
- Référence CVE CVE-2009-1834 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1834>

- Référence CVE CVE-2009-1835 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1835>
- Référence CVE CVE-2009-1836 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1836>
- Référence CVE CVE-2009-1837 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1837>
- Référence CVE CVE-2009-1838 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1838>
- Référence CVE CVE-2009-1839 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1839>
- Référence CVE CVE-2009-1840 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1840>
- Référence CVE CVE-2009-1841 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1841>

Gestion détaillée du document

12 juin 2009 version initiale.