

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-048>

Gestion du document

Référence	CERTA-2009-AVI-048
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	04 février 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité Mozilla 2009-01 à 2009-06 du 03 février 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 ;
- élévation de privilèges.

2 Systèmes affectés

Toutes les versions de Firefox 3 antérieures à la version 3.0.6.

3 Résumé

Plusieurs vulnérabilités affectent Mozilla Firefox et permettent à une personne malintentionnée de réaliser un grand nombre d'actions malveillantes dont exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été découvertes dans Mozilla Firefox :

- plusieurs erreurs dans la gestion de la mémoire permettent de réaliser un déni de service ou une exécution de code arbitraire à distance ;
- une vulnérabilité affectant une méthode *chrome XLB* permet d'exécuter du code *JavaScript* malveillant ;
- une erreur dans le système de restauration des sessions permet à une personne malintentionnée de récupérer des données dans un fichier stocké en local lors de la réouverture des onglets sauvegardés ;
- un contournement de la vulnérabilité corrigée dans le bulletin *MFSA2008-47* permet à une personne malveillante d'injecter du code arbitraire dans un document *chrome* et de l'exécuter avec les privilèges *chrome* ;
- un contournement de la protection *HTTPOnly* permet de lire des fichiers de session via un code *JavaScript* utilisant certaines *API* ;
- certaines directives *HTTP* de non mise en cache ne sont pas respectées par le navigateur et permettent de porter atteinte à la confidentialité de données personnelles lorsque le système est partagé entre plusieurs utilisateurs.

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 MFSA2009-01 du 03 février 2009 :
<http://www.mozilla.org/security/announce/2009/MFSA2009-01.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-02 du 03 février 2009 :
<http://www.mozilla.org/security/announce/2009/MFSA2009-02.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-03 du 03 février 2009 :
<http://www.mozilla.org/security/announce/2009/MFSA2009-03.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-04 du 03 février 2009 :
<http://www.mozilla.org/security/announce/2009/MFSA2009-04.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-05 du 03 février 2009 :
<http://www.mozilla.org/security/announce/2009/MFSA2009-05.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2009-06 du 03 février 2009 :
<http://www.mozilla.org/security/announce/2009/MFSA2009-06.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2008-47 du 12 novembre 2008 :
<http://www.mozilla.org/security/announce/2008/MFSA2008-47.html>
- Référence CVE CVE-2009-0352 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0352>
- Référence CVE CVE-2009-0353 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0353>
- Référence CVE CVE-2009-0354 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0354>
- Référence CVE CVE-2009-0355 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0355>
- Référence CVE CVE-2009-0356 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0356>
- Référence CVE CVE-2009-0357 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0357>
- Référence CVE CVE-2009-0358 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0358>

Gestion détaillée du document

04 février 2009 version initiale.