



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 août 2009
N° CERTA-2009-AVI-306

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-306>

Gestion du document

Référence	CERTA-2009-AVI-306
Titre	Vulnérabilités dans Firefox
Date de la première version	04 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla 2009/mfsa2009-42 à 44
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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Firefox 3.0.x et 3.5.x.

3 Résumé

Plusieurs vulnérabilités affectent le navigateur Firefox et permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités affectent le navigateur Firefox :

- la différence de traitement des noms d'hôtes contenant un caractère *null* illégal par les autorités de certification, lors de la demande de certificat par le serveur, et par le navigateur, lors de l'établissement d'une session

SSL, permet à un utilisateur malveillant de lire ou de modifier des données dans une transaction sécurisée par SSL. Cette vulnérabilité permet à utilisateur malveillant d'exécuter du code arbitraire à distance au travers du système de mise à jour ;

- le traitement d'expression régulière dans les certificats de clefs publiques restait compatible avec celui des navigateurs Netscape. Ce traitement laxiste permet à un utilisateur malveillant d'exécuter du code arbitraire à distance en présentant au navigateur un certificat spécialement conçu ;
- le contenu de la barre d'adresse peut ne pas être conforme au contenu de la fenêtre principale. Cette vulnérabilité permet à un utilisateur malveillant de contourner la politique de sécurité en trompant l'utilisateur sur l'identité du site sur lequel il navigue.

5 Solution

Les versions 3.5.2 et 3.0.13 corrigent ces vulnérabilités.

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/mfsa2009-42 du 01 août 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-42.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-43 du 01 août 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-43.html>
- Bulletin de sécurité de la fondation Mozilla 2009/mfsa2009-44 du 03 août 2009 :
<http://www.mozilla.org/security/announce/2009/mfsa2009-44.html>
- Référence CVE CVE-2009-2404 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2404>
- Référence CVE CVE-2009-2408 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2408>
- Référence CVE CVE-2009-2654 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2654>

Gestion détaillée du document

04 août 2009 version initiale.