Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 mars 2009
N° CERTA-2009-AVI-086

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Firefox

Gestion du document

Référence	CERTA-2009-AVI-086
Titre	Vulnérabilités de Firefox
Date de la première version	05 mars 2009
Date de la dernière version	–
Source(s)	Bulletins de sécurité de la fondation Mozilla du 04 mars 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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Firefox 2.x et 3.x.

3 Résumé

Plusieurs vulnérabilités affectent le navigateur Firefox. Certaines d'entre elles permettent à un utilisateur malveillant d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Plusieurs vulnérabilités sont présentes dans le navigateur Firefox :

- des erreurs dans la bibliothèque de traitement des images au format PNG permettent à un utilisateur malveillant de provoquer l'arrêt du navigateur ou d'exécuter du code arbitraire à distance ;

- le moteur de mise en page comporte plusieurs défauts qui permettent à un utilisateur malveillant de réaliser un déni de service à distance ;
- le moteur JavaScript comporte une vulnérabilité exploitable par un utilisateur malveillant pour réaliser un déni de service à distance ;
- un problème dans la gestion de la mémoire permet à un utilisateur malveillant d'exécuter du code arbitraire à distance ;
- un traitement défectueux permet à un site malveillant de lire sans autorisation des informations au format XML provenant d'un autre domaine ;
- une erreur dans le traitement des caractères de contrôle permet à un utilisateur malveillant d'afficher dans la barre d'adresses une adresse réticulaire qui ne correspond pas à l'adresse réelle.

5 Solution

La branche 2.x de Firefox n'est plus maintenue depuis le 18 décembre 2008.

La version 3.0.7 de Firefox corrige 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 MFSA2009-07 du 04 mars 2009 : http://www.mozilla.org/security/announce/2009/MFSA2009-07.html
- Bulletin de sécurité de la fondation Mozilla MFSA2009-08 du 04 mars 2009 : http://www.mozilla.org/security/announce/2009/MFSA2009-08.html
- Bulletin de sécurité de la fondation Mozilla MFSA2009-09 du 04 mars 2009 : http://www.mozilla.org/security/announce/2009/MFSA2009-09.html
- Bulletin de sécurité de la fondation Mozilla MFSA2009-10 du 04 mars 2009 : http://www.mozilla.org/security/announce/2009/MFSA2009-10.html
- Bulletin de sécurité de la fondation Mozilla MFSA2009-11 du 04 mars 2009 : http://www.mozilla.org/security/announce/2009/MFSA2009-11.html
- Référence CVE CVE-2009-0040 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0040
- Référence CVE CVE-2009-0771 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0771
- Référence CVE CVE-2009-0772 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0772
- Référence CVE CVE-2009-0773 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0773
- Référence CVE CVE-2009-0774 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0774
- Référence CVE CVE-2009-0775 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0775
- Référence CVE CVE-2009-0776 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0776
- Référence CVE CVE-2009-0777 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0777

Gestion détaillée du document

05 mars 2009 version initiale.