



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 novembre 2007
N° CERTA-2007-AVI-509-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2007-AVI-509>

Gestion du document

Référence	CERTA-2007-AVI-509-001
Titre	Vulnérabilités dans Mozilla Firefox
Date de la première version	27 novembre 2007
Date de la dernière version	30 novembre 2007
Source(s)	Avis de sécurité Mozilla MFSA du 26 novembre 2007
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Mozilla Firefox version 2.0.0.9 ainsi que celles antérieures ;
- Netscape Navigator versions 9.0.0.3 et antérieures.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le navigateur Mozilla Firefox. Exploitées, elles permettraient à une personne malveillante d'exécuter du code sur le système vulnérable, ou conduire des attaques par injection de code indirecte de type CSRF (*Cross-Site Request Forgery*) ou XSS.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le navigateur Mozilla Firefox :

1. l'une d'elles a été présentée dans le bulletin d'actualité CERTA-2007-ACT-045 du 09 novembre 2007, et implique les URI de la forme `jar :`. Des fichiers archivés se trouvant sur un site web (par défaut, ou après un téléchargement) peuvent être exploités pour lancer des attaques par injection de code indirecte (XSS). Le correctif limite l'usage de ces URI par un en-tête `Content-Type` de forme `application/java-archive` et `application/x-jar`. Il s'agit donc d'une mesure de correction partielle.
2. une vulnérabilité permet de tricher sur le champ `Referer` de l'en-tête HTTP. Celle-ci peut être exploitée pour lancer des attaques de type CSRF (*Cross-Site Request Forgery*), en remplaçant sa valeur légitime et après une situation de compétition particulière.
3. trois autres vulnérabilités sont citées par Mozilla. Elles provoqueraient une corruption de la mémoire, et permettraient éventuellement d'exécuter des commandes arbitraires sur un système vulnérable. Elles concernent notamment l'interprétation d'images PNG et la méthode `destructor` XBL.

5 Solution

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

6 Documentation

- Document du CERTA CERTA-2007-ACT-045 du 09 novembre 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-045.pdf>
- Bulletin de sécurité de la fondation Mozilla MFSA2007-37 du 26 novembre 2007 :
<http://www.mozilla.org/security/announce/2007/mfsa2007-37.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2007-38 du 26 novembre 2007 :
<http://www.mozilla.org/security/announce/2007/mfsa2007-38.html>
- Bulletin de sécurité de la fondation Mozilla MFSA2007-39 du 26 novembre 2007 :
<http://www.mozilla.org/security/announce/2007/mfsaA2007-39.html>
- Mise à jour de Netscape Navigator :
<http://browser.netscape.com/downloads/>
- Référence CVE CVE-2007-5947 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5947>
- Référence CVE CVE-2007-5959 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5959>
- Référence CVE CVE-2007-5960 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5960>

Gestion détaillée du document

27 novembre 2007 version initiale ;

30 novembre 2007 ajout des références à Netscape.