Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 août 2007
N° CERTA-2007-AVI-318-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Mozilla Firefox

Gestion du document

Référence	CERTA-2007-AVI-318-001
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	18 juillet 2007
Date de la dernière version	27 août 2007
Source(s)	Bulletin de mises à jour Mozilla du 18 juillet 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Les versions de Mozilla Firefox antérieures à 2.0.0.5.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans Mozilla Firefox. Elles ont fait l'objet de l'alerte CERTA-2007-ALE-012. L'exploitation de celles-ci peuvent conduire une personne malveillante à exécuter du code arbitraire, à interrompre le service, ou à récupérer des informations confidentielles sur le système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans Mozilla Firefox. Elles ont fait l'objet de l'alerte CERTA-2007-ALE-012. Parmi celles-ci :

- le navigateur pourrait sous certaines conditions se fermer, ou dysfonctionner, suite à des corruptions de mémoire possibles ;
- une situation de compétition existerait entre les deux fonctions `addEventListener` et `setTimeout`. L'exploitation de celle-ci permettrait d'injecter du code, de manière indirecte, dans le contexte d'un autre site (attaque XSS) ;
- une situation de compétition permettrait de modifier le contenu des cadres `about:blank` de la page. L'exploitation de cette vulnérabilité modifie l'apparence d'un site, dans le cadre d'attaques par filoutage par exemple ;
- il est possible d'appeler les fonctions de manipulation d'événements pour des éléments qui sont indépendants du document, ce qui laisse l'opportunité à des personnes malveillantes d'exécuter des commandes arbitraires avec les droits `chrome` ;
- l'interprétation de certaines adresses réticulaires comprenant le caractère `%00` ne serait pas cohérente avec celle effectuée par Microsoft. Cette vulnérabilité permet ainsi à une personne locale au système d'exécuter des programmes avec des privilèges plus élevés, comme ceux de l'administrateur ;
- il est possible d'appeler Firefox par le biais d'Internet Explorer. Ce problème a été décrit en particulier dans le bulletin d'actualité CERTA-2007-ACT-028 ;
- il est possible de contourner la politique du navigateur qui vérifie la cohérence entre les sources des éléments (*Same-Origin Policy*), en accédant à certaines données en cache par le biais de la commande `wyciwyg://`. Une personne malveillante peut ainsi avoir accès à des informations confidentielles ou corrompre les fichiers en cache ;
- il serait possible, par le biais du navigateur, de modifier `XPCNativeWrapper` afin d'exécuter à la place un code arbitraire.

5 Solution

Se référer au bulletin de sécurité de l'éditeur Mozilla pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Les avis de sécurité Mozilla :
  http://www.mozilla.org/projects/security/known-vulnerabilities.html#firefox2.0.0.5
- Bulletin de sécurité Gentoo GLSA-200708-09 du 14 août 2007 :
  http://www.gentoo.org/security/en/glsa/glsa-200708-09.xml
- Bulletin de sécurité Mandriva MDKSA-2007:152 du 01 août 2007 :
  http://www.mandriva.com/security/advisories?name=MDKSA-2007:152
- Bulletin de sécurité Debian DSA-1337 du 22 juillet 2007 :
  http://www.debian.org/security/2007/dsa-1337
- Bulletin de sécurité Debian DSA-1338 du 23 juillet 2007 :
  http://www.debian.org/security/2007/dsa-1338
- Bulletin de sécurité Debian DSA-1339 du 23 juillet 2007 :
  http://www.debian.org/security/2007/dsa-1339
- Bulletin de sécurité Red Hat RHSA-2007:0722 du 18 juillet 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0722.html
- Bulletin de sécurité Red Hat RHSA-2007:0723 du 18 juillet 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0723.html
- Bulletin de sécurité Red Hat RHSA-2007:0724 du 18 juillet 2007 :
  http://rhn.redhat.com/errata/RHSA-2007-0724.html
- Bulletin de sécurité Ubuntu USN-490-1 du 19 juillet 2007 :
  http://www.ubuntu.com/usn/usn-490-1

- Bulletin de sécurité Ubuntu USN-503-1 du 24 août 2007 : http://www.ubuntu.com/usn/usn-503-1
- Bulletin de sécurité SuSE SUSE-SR:2007:049 du 02 août 2007 : http://lists.opensuse.org/opensuse-security-announce/2007-08/msg00002.html
- Avis de sécurité Mozilla MFSA2007-18 du 17 juillet 2007 : http://www.mozilla.org/security/announce/2007/mfsa2007-18.html
- Avis de sécurité Mozilla MFSA2007-19 du 17 juillet 2007 : http://www.mozilla.org/security/announce/2007/mfsa2007-19.html
- Avis de sécurité Mozilla MFSA2007-20 du 17 juillet 2007 : http://www.mozilla.org/security/announce/2007/mfsa2007-20.html
- Avis de sécurité Mozilla MFSA2007-21 du 17 juillet 2007 : http://www.mozilla.org/security/announce/2007/mfsa2007-21.html
- Avis de sécurité Mozilla MFSA2007-22 du 17 juillet 2007 : http://www.mozilla.org/security/announce/2007/mfsa2007-22.html
- Avis de sécurité Mozilla MFSA2007-23 du 17 juillet 2007 : http://www.mozilla.org/security/announce/2007/mfsa2007-23.html
- Avis de sécurité Mozilla MFSA2007-24 du 17 juillet 2007 : http://www.mozilla.org/security/announce/2007/mfsa2007-24.html
- Avis de sécurité Mozilla MFSA2007-25 du 17 juillet 2007 : http://www.mozilla.org/security/announce/2007/mfsa2007-25.html
- Référence CVE CVE-2007-3089 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3089
- Référence CVE CVE-2007-3285 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3285
- Référence CVE CVE-2007-3656 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3656
- Référence CVE CVE-2007-3670 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3670
- Référence CVE CVE-2007-3734 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3734
- Référence CVE CVE-2007-3735 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3735
- Référence CVE CVE-2007-3736 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3736
- Référence CVE CVE-2007-3737 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3737
- Référence CVE CVE-2007-3738 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3738

Gestion détaillée du document

18 juillet 2007 version initiale.
27 août 2007 ajout des références aux bulletins de sécurité Gentoo, Debian, Mandriva, Red Hat, SuSE et Ubuntu.