Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 juillet 2007
N° CERTA-2007-ALE-012-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Multiples vulnérabilités dans Mozilla Firefox

Gestion du document

Référence	CERTA-2007-ALE-012-003
Titre	Multiples vulnérabilités dans Mozilla Firefox
Date de la première version	06 juin 2007
Date de la dernière version	18 juillet 2007
Source(s)	
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 la confidentialité des données.

2 Systèmes affectés

Firefox versions 2.0.0.4 et antérieures.

3 Résumé

Plusieurs vulnérabilités sont présentes dans `Mozilla Firefox` et permettent à un utilisateur distant de porter atteinte à la confidentialité des données ou potentiellement d'exécuter du code arbitraire sur la machine vulnérable.

4 Description

Plusieurs vulnérabilités dont certaines ont déjà été abordées dans nos bulletins d'actualités sont présentes dans le navigateur `Mozilla Firefox`:

– une première concerne une erreur mal corrigée relative au contexte de navigation `ressource://` qui

permettrait un accès à certains fichiers de la machine vulnérable. Un article dans le bulletin d'actualité CERTA-2007-ACT-020 détaille cette vulnérabilité. Il est à noter que la faille n'est que partiellement corrigée et permet encore l'accès à certains fichiers.

– une seconde concerne le système de mise à jour des extensions dans `Firefox`. Un manque de contrôle dans la manière dont les mises à jour des extensions sont effectuées permet l'utilisation de protocoles non-sûrs. Les détails de cette faille sont présentés dans CERTA-2007-ACT-022.
– une troisième et dernière vulnérabilité plus récente se rapporte à la gestion des `IFRAMES` et permettrait d'associer une gestion arbitraire d'événements comme des frappes claviers dans le contexte d'une page particulière. Ainsi, il serait possible de capturer des éléments fournis par un utilisateur dans un formulaire et cela à son insu.
– une quatrième vulnérabilité est dûe au fait que `Firefox` ne filtre pas correctement les extensions des fichiers qui lui sont fournis en `URL`. Il est ainsi possible de modifier le comportement de `Firefox` vis-à-vis d'un fichier par le biais d'une extension construite de façon particulière. Cette faille permet donc à un utilisateur malveillant d'exécuter du code arbitraire à distance.

5 Contournement provisoire

De façon générale et en particulier pour la troisième vulnérabilité, il est fortement recommandé de désactiver par défaut le support des `Javascript` dans `Firefox`.
L'accumulation de vulnérabilités dans Firefox peut rendre également préférable l'utilisation d'un navigateur alternatif autre que ceux basés sur le moteur de rendu de `Firefox : Gecko`.

6 Solution

Se reporter à la mise à jour de Mozilla Firefox, version 2.0.0.5, publiée le 17 juillet 2007, et détaillée dans l'avis CERTA-2007-AVI-318.

7 Documentation

– Avis du CERTA CERTA-2007-AVI-318 du 18 juillet 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-318
– Bulletin d'actualité CERTA-2007-ACT-020 du 18 mai 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-020.pdf
– Bulletin d'actualité CERTA-2007-ACT-022 du 01 juin 2007 :
http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-022.pdf
– Rapport de coquille Mozilla #381300 :
https://bugzilla.mozilla.org/show_bug.cgi?id=381300
– Rapport de coquille Mozilla #382686 :
https://bugzilla.mozilla.org/show_bug.cgi?id=382686
– Références CVE :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3072
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3073
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3074
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3089

Gestion détaillée du document

06 juin 2007 version initiale ;
08 juin 2007 ajout de la quatrième vulnérabilité relative aux extensions de fichiers ;
13 juin 2007 ajout des références CVE.
18 juillet 2007 ajout de la section `Solution`, suite à la publication de la nouvelle version 2.0.0.5 de Firefox.