



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 juillet 2007
N° CERTA-2007-ALE-013-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité 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-ALE-013>

Gestion du document

Référence	CERTA-2007-ALE-013-003
Titre	Vulnérabilité dans Mozilla Firefox
Date de la première version	27 juillet 2007
Date de la dernière version	31 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 commandes arbitraires à distance.

2 Systèmes affectés

Les navigateurs utilisant le moteur de rendu de Mozilla (Gecko) sont vulnérables sur Microsoft Windows XP SP2, notamment :

- Mozilla Firefox 2.0.0.5 ;
- Netscape Navigator 9.

3 Résumé

Une vulnérabilité dans le traitement de certaines URI sous Mozilla Firefox sur Windows XP SP2 permet à une personne malintentionnée d'exécuter des commandes arbitraires à distance.

4 Description

Une vulnérabilité a été identifiée concernant Mozilla Firefox fonctionnant sur des systèmes Windows XP SP2 sur lesquels Internet Explorer 7 est installé. Il n'est pas exclu que d'autres systèmes d'exploitation et navigateurs soient impactés.

Par le biais d'une URI spécifiquement construite, un attaquant peut faire en sorte que le traitement d'URI applicatives (par exemple `mailto:`, `news:`, `nntp:`, `snews`) soit réalisé comme celui d'une URI de type `FileType`. Une personne malintentionnée peut ainsi exécuter des commandes arbitraires à distance via des liens malveillants.

Des preuves de faisabilité ont été publiées sur l'Internet et peuvent être trivialement modifiées pour effectuer des actions malveillantes.

5 Contournement provisoire

5.1 Pour les utilisateurs

Le contournement provisoire consiste à désactiver l'appel par Mozilla Firefox d'applications externes pour mettre en œuvre certains protocoles.

- dans la barre d'adresse de Firefox, taper `about:config` ;
- dans le filtre, taper `protocol` pour obtenir la liste des options utiles ;
- mettre les valeurs `network.protocol-handler.external.XX` (eg. `network.protocol-handler.external.snews`) ainsi que `network.protocol-handler.external-default` à "false" en double cliquant dessus ;

Un autre contournement moins contraignant consiste à forcer l'affichage d'avertissements en fixant les champs `network.protocol-handler.warn-external.XX` à "true".

Le CERTA rappelle également l'importance de vérifier les liens, de cliquer avec précaution, ou de taper manuellement l'adresse. Il est aussi recommandé de lancer le navigateur avec un utilisateur disposant de privilèges limités.

5.2 Pour les administrateurs

Le contournement consiste à bloquer tout trafic utilisant des URI non classiques (en général, tout sauf `http:`, `https:`, `ftp:`). Il peut être possible de coupler ce filtre en le limitant aux navigateurs utilisant le moteur de rendu Gecko (filtrer sur le `referrer`).

6 Solution

Se reporter à la mise à jour de Mozilla Firefox, version 2.0.0.6, publiée le 30 juillet 2007 et détaillée dans l'avis CERTA-2007-AVI-337.

7 Documentation

- Avis du CERTA CERTA-2007-AVI-337 du 31 juillet 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-338/index.html>
- Rapport de coquille Mozilla #389580 du 25 juillet 2007 :
https://bugzilla.mozilla.org/show_bug.cgi?id=389580
- Bulletin de l'US CERT VU#783400 du 26 juillet 2007 :
<http://www.kb.cert.org/vuls/id/783400>
- Bulletin de l'US CERT VU#403150 du 27 juillet 2007 :
<http://www.kb.cert.org/vuls/id/403150>
- Bulletin d'actualité CERTA-2007-ACT-030 du 27 juillet 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-030.pdf>

Gestion détaillée du document

27 juillet 2007 version initiale ;

30 juillet 2007 mise à jour du contournement provisoire pour utilisateurs ;

30 juillet 2007 mise à jour du contournement provisoire pour administrateurs et ajout d'une référence ;

31 juillet 2007 ajout de la section solution suite à la publication de la nouvelle version 2.0.0.6 de Firefox.