Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 septembre 2007
N° CERTA-2007-AVI-407

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Firefox

Gestion du document

Référence	CERTA-2007-AVI-407
Titre	Vulnérabilité dans Firefox
Date de la première version	19 septembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Mozilla MFSA2007-28 du 18 septembre 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 2.0.0.6 ainsi que celles antérieures.

3 Résumé

Une vulnérabilité a été identifiée dans le navigateur Mozilla Firefox, en relation avec l'alerte CERTA-2007-ALE-014. L'exploitation de cette dernière permet à des fichiers, notamment au format QuickTime de lancer le navigateur par défaut en ligne de commandes avec des options arbitraires. La politique de sécurité configurée dans le navigateur est alors contournée.

4 Description

Une vulnérabilité a été identifiée dans le navigateur Mozilla Firefox, en relation avec l'alerte CERTA-2007-ALE-014. L'exploitation de cette dernière permet à des fichiers, notamment au format QuickTime (`qtl`) de lancer

le navigateur par défaut en ligne de commandes avec des options arbitraires. Ainsi, l'option `-chrome` permet de lancer des scripts de commandes sur le système avec les droits de l'utilisateur. La politique de sécurité configurée dans le navigateur est alors contournée, cette vulnérabilité pouvant être utilisée pour installer et exécuter tout code arbitraire sur le système vulnérable.

Le correctif proposé par Mozilla bloque ainsi l'exécution de script arbitraire depuis la ligne de commandes.

5 Solution

Se référer au bulletin de sécurité MFSA2007-028 de Mozilla pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Mozilla MFSA2007-028 du 18 septembre 2007 :
  http://www.mozilla.org/security/announce/2007/mfsa2007-28.html
- Alerte CERTA-2007-ALE-014 du 14 septembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-014/

Gestion détaillée du document

19 septembre 2007 version initiale.