Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 octobre 2007
N° CERTA-2007-ALE-014-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Apple QuickTime

Gestion du document

Référence	CERTA-2007-ALE-014-003
Titre	Vulnérabilité dans Apple QuickTime
Date de la première version	13 septembre 2007
Date de la dernière version	12 octobre 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.

2 Systèmes affectés

Apple QuickTime 7.2 et versions antérieures sur Microsoft Windows.

3 Résumé

Une vulnérabilité touchant `Apple QuickTime` permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité a été identifiée dans `Apple QuickTime`. Ce lecteur multimédia permet à une personne de spécifier un média à lire après l'exécution du média courant (option `QTNEXT` d'un fichier multimédia). Cette fonctionnalité peut cependant être détournée pour exécuter du code `Javascript`, et donc du code arbitraire sur le poste de l'utilisateur. L'interpréteur `Javascript` utilisé est le navigateur Internet par défaut de l'utilisateur.

Des codes de démonstration sont disponibles sur l'Internet et fonctionnent si Mozilla Firefox est le navigateur par défaut, sur Microsoft Windows. Les autres systèmes d'exploitation ne semblent pas concernés mais le navigateur Netscape Navigator, basé sur le même moteur de rendu que Firefox, est aussi vulnérable.

Pour résumer, les problèmes rencontrés sont :

- QuickTime n'offre pas la possibilité de bloquer le Javascript ;
- QuickTime associé à un navigateur comme Mozilla Firefox ne respecte pas la politique du navigateur liée au Javascript.

Il est important de noter que l'utilisation d'un navigateur alternatif ne contourne pas le problème si Mozilla Firefox est défini comme navigateur par défaut.

5 Contournements provisoires

Quelques contournements sont envisageables :

1° – ouvrir la fenêtre about:config ;
– filtrer les options en tapant protocol ;
– mettre l'option network.protocol-handler.external.javascript à la valeur true.
Ceci n'empêche pas l'exploitation mais avertit l'utilisateur lorsqu'une application externe appelle l'interpréteur Javascript de Firefox.

2° l'utilisation d'une extension telle que NoScript peut bloquer l'exécution de code si l'option *Forbid scripts globally* est activée.

3° définir un navigateur alternatif non basé sur le moteur de rendu Gecko comme navigateur par défaut. Des tests internes au CERTA ont montré que Seamonkey 1.1.4 ne semble pas vulnérable mais il convient de rester prudent.

Le meilleur contournement à la date de rédaction de cette alerte consiste à désinstaller complètement l'application QuickTime dans l'attente d'un correctif d'Apple et/ou Mozilla.

6 Solution

L'éditeur Mozilla a publié un correctif pour le navigateur Firefox (version 2.0.0.7) qui empêche l'exécution de scripts arbitraires via une ligne de commande avec le paramètre -chrome.

Apple a également publié un correctif (7.2.0.245) pour Quicktime. (cf. section Documentation).

7 Documentation

- Avis du CERTA CERTA-2007-AVI-407 du 19 septembre 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-407/index.html
- Référence CVE CVE-2006-4965 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4965
- Référence CVE CVE-2007-4673 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4673
- Bulletin de sécurité Apple 306560 du 03 octobre 2007 :
  http://docs.info.apple.com/article.html?artnum=306560
- Bulletin de sécurité Mozilla MFSA 2007-28 du 18 septembre 2007 :
  http://www.mozilla.org/security/announce/2007/mfsa2007-28.html
- Entrée sur le bloc-notes Mozilla du 12 septembre 2007 :
  http://blog.mozilla.com/security/2007/09/12/quicktime-to-firefox-issue
- Rapport de bogue #395942 de Mozilla :
  https://bugzilla.mozilla.org/show_bug.cgi?id=395942
- Bulletin d'actualité CERTA-2007-ACT-037 - « Vulnérabilité sur Quicktime et Firefox » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-037.pdf
- Bulletin d'actualité CERTA-2007-ACT-011 - « Le Javascript est omniprésent » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-011.pdf

Gestion détaillée du document

13 septembre 2007 version initiale ;
14 septembre 2007 mise à jour des systèmes affectés, de la description, des contournements et ajout de références ;
19 septembre 2007 mise à jour de la solution et de la documentation ;
12 octobre 2007 ajout d'une référence CVE et du correctif pour Quicktime.