Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 septembre 2010
N° CERTA-2010-ALE-013-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans le contrôle ActiveX Apple QuickTime

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-2010-ALE-013`

Gestion du document

Référence	CERTA-2010-ALE-013-001
Titre	Vulnérabilité dans le contrôle ActiveX Apple QuickTime
Date de la première version	31 août 2010
Date de la dernière version	17 septembre 2010
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 versions 7.6.7 et antérieures sur plateforme Windows.

3 Résumé

Une vulnérabilité non-corrigée dans le contrôle ActiveX `Apple QuickTime` permet à un utilisateur distant malintentionné d'exécuter du code arbitraire.

4 Description

Une vulnérabilité non-corrigée dans le contrôle `ActiveX QuickTime` (*QTPlugin.ocx*) permet à une personne distante malintentionnée d'exécuter du code arbitraire via une page web spécialement construite.

Le problème résidant dans le contrôle `ActiveX QuickTime`, l'exploitation n'est possible, à ce jour, que via le navigateur `Internet Explorer`.

Le savoir-faire nécessaire pour exploiter cette vulnérabilité est d'ores et déjà disponible sur l'Internet.

5 Contournement provisoire

Afin de limiter l'impact lié à l'exploitation de cette vulnérabilité, les contournements décrits ci-dessous, non exhaustifs, peuvent être appliqués.

Remarque : la mise en œuvre de ces contournements de sécurité peut avoir des effets de bord sur l'activité du système. Il est important de les tester avant tout déploiement.

- Renommer, supprimer, ou retirer les droits d'accès du fichier suivant :

  ```
  C:\Program Files\QuickTime\QTPlugin.ocx
  ```

- désactiver le chargement du contrôle ActiveX dans Internet Explorer :
  Positionner la valeur `Compatibility Flags` comme décrit ci-dessous :

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\
  {02BF25D5-8C17-4B23-BC80-D3488ABDDC6B}]
  ``Compatibility Flags''=dword:00000400
  ```

6 Solution

Cette vulnérabilité est corrigée dans la version 7.6.8 de *QuickTime*. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Apple HT4339 du 15 septembre 2010 :
  http://support.apple.com/kb/HT4339
- Avis CERTA-2010-AVI-441 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-441/
- Référence CVE-2010-1818 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1818

Gestion détaillée du document

31 août 2010 version initiale.

17 septembre 2010 publication du correctif.