Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 juin 2007
N° CERTA-2007-AVI-277

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités dans Apple MacOS X

Gestion du document

Référence	CERTA-2007-AVI-277
Titre	Plusieurs vulnérabilités dans Apple MacOS X
Date de la première version	26 juin 2007
Date de la dernière version	–
Source(s)	Mise à jour de sécurité Apple 2007-006 du 21 juin 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- MacOS X v10.3.9 ;
- MacOS X Server v10.3.9 ;
- MacOS X v10.4.9 ou une version plus ancienne ;
- MacOS X Server v10.4.9 ou une version plus ancienne.

3 Résumé

Deux vulnérabilités ont été identifiées dans le système d'exploitation MacOS X. Leur exploitation, par le biais d'une navigation sur une page malveillante, peut entraîner une injection de code indirecte (*cross-site scripting*), un dysfonctionnement de l'application voire l'exécution de code arbitraire sur le système vulnérable.

4 Description

Deux vulnérabilités ont été identifiées dans le système d'exploitation MacOS X.

- `WebCore`, et en particulier `XMLHttpRequest` ne manipulerait pas correctement certaines requêtes HTTP. Cette vulnérabilité pourrait amener un utilisateur naviguant sur une page malveillante à conduire une attaque par injection de code indirecte (*cross-site scripting*) ;
- `WebKit` ne convertirait pas correctement certains types au cours du rendu des cadres dans une page, pouvant provoquer une corruption de la mémoire. Cette vulnérabilité peut être exploitée par le biais d'une page Web spécialement construite : celle-ci provoquerait un dysfonctionnement de l'application voire l'exécution de code arbitraire sur le système vulnérable.

5 Solution

Se référer au bulletin de sécurité 2007-006 de l'éditeur Apple pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple du 21 juin 2007 :
  http://docs.info.apple.com/article.html?artnum=305759
- Référence CVE CVE-2007-2399 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2399
- Référence CVE CVE-2007-2401 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2401

Gestion détaillée du document

26 juin 2007 version initiale.