Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 mars 2006
N° CERTA-2006-AVI-108

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans MacOS

Gestion du document

Référence	CERTA-2006-AVI-108
Titre	Multiples vulnérabilités dans MacOS
Date de la première version	14 mars 2006
Date de la dernière version	–
Source(s)	Mise à jour sécurité de l'éditeur Apple
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Mac OS X version 10.4.5
- Mac OS X Server version 10.4.5

3 Description

De multiples vulnérabilités existent dans la version actuelle de Mac 0S X v.10.4.5. Parmi les services impactés, nous notons :

- `Mail` : Une personne malveillante peut envoyer un courriel particulier avec pièces jointes, afin d'inciter l'utilisateur à ouvrir celles-ci. Cette action peut entraîner un dépassement de tampon permettant l'exécution de code arbitraire sur le système. Le problème n'existe pas pour les versions Mac OS antérieures à 10.4.

- `Safari, LaunchServices` : Safari ouvre automatiquement des fichiers courants, comme les images ou les vidéos. Une personne malveillante peut alors insérer sur son site un code ayant une telle apparence, afin d'exécuter un code arbitraire à distance. Le problème n'existe pas pour les versions de Mac OS antérieures à 10.4.
- `CoreTypes` : Une page contenant un code `JavaScript` malveillant permet d'accéder et modifier des documents d'origine différente (voir la notion sous Mac OS de `Same-Origin`, une origine étant un triplet constitué par le protocole, le port et le serveur Internet).

4 Solution

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

5 Documentation

- Bulletin de sécurité Apple du 13 mars 2006 :
  http://docs.info.apple.com/article.html?artnum=303453
- Référence CVE CVE-2006-0400 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0400
- Référence CVE CVE-2006-0396 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0396
- Référence CVE CVE-2006-0397 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0397
- Référence CVE CVE-2006-0398 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0398
- Référence CVE CVE-2006-0399 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0399

Gestion détaillée du document

14 mars 2006 version initiale.