Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 octobre 2006
N° CERTA-2006-AVI-416

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Plusieurs vulnérabilités dans Apple Mac OS X et des applications associées

Gestion du document

Référence	CERTA-2006-AVI-416
Titre	Plusieurs vulnérabilités dans Apple Mac OS X et des applications associées
Date de la première version	03 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple 2006-006 du 29 septembre 2006
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 ;
- élévation de privilèges.

2 Systèmes affectés

- Apple Mac OS X version 10.3.9 ;
- Apple Mac OS X Server version 10.3.9 ;
- Apple Mac OS X v10.4 , pour les versions antérieures à 10.4.8 ;
- Apple Mac OS X Server v10.4, pour les versions antérieures à 10.4.8.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le système d'exploitation Apple Mac OS X, ainsi que certaines applications associées à ce système, telles que Adobe Flash Player, Safari ou QuickDraw. L'exploitation de ces vulnérabilités peut permettre à une personne malveillante d'élever ses privilèges localement, voire d'exécuter des commandes arbitraires à distance.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le système d'exploitation Apple Mac OS X, ainsi que certaines applications associées à ce système. Parmi celles-ci :

- une vulnérabilité dans `CFNetwork`, une interface de programmation permettant l'abstraction de certaines fonctionnalités des couches réseau : elle ne manipulerait pas correctement les authentifications SSL. Tout client s'appuyant sur elle, comme le navigateur `Safari`, pourrait donc montrer une connexion SSL authentifiée et chiffrée (icône *cadenas* dans la fenêtre du navigateur), bien que l'authentification ne soit pas effectuée.
- plusieurs vulnérabilités dans l'application `Adobe Flash Player`, aussi commentées dans l'avis du CERTA CERTA-2006-AVI-398 : celle-ci ne manipulerait pas convenablement certains fichiers multimedia au format `.swf`, permettant à un document spécialement construit de contourner le paramètre de sécurité nommé `allowScriptAccess` de l'application vulnérable.
- une vulnérabilité dans l'application `ImageIO` : elle n'interprèterait pas correctement certaines images `JPEG2000`. Une personne malveillant pourrait construire un document particulier exploitant cette vulnérabilité, afin d'exécuter du code arbitraire lorsque l'image est visualisée sur le système vulnérable.
- une vulnérabilité dans la manipulation des erreurs par le noyau de Mac OS X : quand une erreur survient (fermer une application brutalement par exemple), le noyau fait appel à des ports d'exception `Mach`. Une personne malveillante pourrait profiter des droits accordés à ces derniers pour élever ses privilèges à ceux de l'administrateur (`root`).
- plusieurs vulnérabilités dans l'application `LoginWindow` : cette application gère notamment les services autorisés aux utilisateurs qui se connecteraient à distance sur le système. Il serait possible pour une personne malveillante de contourner la politique de contrôle d'accès spécifiée dans le système.
- une vulnérabilité dans le service `Préferences`, servant à configurer le système d'exploitation : les privilèges ne seraient pas correctement nettoyés à la suppression d'un compte administrateur.
- une vulnérabilité non documentée concernant la manipulation d'images `PICT` par l'application `QuickDraw Manager`.
- une vulnérabilité dans le service de messagerie `Cyrus SASL`, au cours de la négaociation DIGEST-MD5 : une personne malveillante pourrait construire un paquet particulier, perturbant le système vulnérable qui le recevrait.
- une vulnérabilité de l'utilitaire `WebCore` : celui-ci est un moteur de rendu HTML pour le système d'exploitation Mac OS X. C'est un des composants primaires repris dans l'utilitaire `WebKit`. Il ne manipulerait pas correctement certains documents au format HTML, permettant à un utilisateur d'exécuter du code sur le système qui ouvrirait son document construit de manière malveillante.
- une vulnérabilité dans le service d'administration `Workgroup Manager`, qui n'utiliserait pas correctement les mots de passe `ShadowHash` avec la hiérarchie des domaines de `NetInfo`.

5 Solution

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

6 Documentation

- Bulletin de sécurité Apple du 29 septembre 2006 :
  http://docs.info.apple.com/article.html?artnum=304460
- Avis du CERTA CERTA-2006-AVI-398, 'Vulnérabilités dans Adobe Flash Player', du 14 septembre 2006 :
  http://www.certa/ssi.gouv.fr/site/CERTA-2006-AVI-398/
- Référence CVE CVE-2006-1721 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1721
- Référence CVE CVE-2006-3311 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3311
- Référence CVE CVE-2006-3587 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3587
- Référence CVE CVE-2006-3588 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3588

- Référence CVE CVE-2006-3946 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3946
- Référence CVE CVE-2006-4387 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4387
- Référence CVE CVE-2006-4390 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4390
- Référence CVE CVE-2006-4391 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4391
- Référence CVE CVE-2006-4392 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4392
- Référence CVE CVE-2006-4393 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4393
- Référence CVE CVE-2006-4394 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4394
- Référence CVE CVE-2006-4395 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4395
- Référence CVE CVE-2006-4397 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4397
- Référence CVE CVE-2006-4399 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4399
- Référence CVE CVE-2006-4640 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4640

Gestion détaillée du document

03 octobre 2006 version initiale.