Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 août 2006
N° CERTA-2006-AVI-317

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Mac OS X

Gestion du document

Référence	CERTA-2006-AVI-317
Titre	Multiples vulnérabilités dans Mac OS X
Date de la première version	02 août 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple du 01/08/2006
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- La version Mac 0S X 10.3.9 ainsi que celles antérieures ;
- la version Mac 0S X 10.3.9 Server ainsi que celles antérieures ;
- la version Mac 0S X 10.4.7 (PPC et Intel) ainsi que celles antérieures ;
- la version Mac 0S X 10.4.7 Server (PPC et Intel) ainsi que celles antérieures.

3 Résumé

De nombreuses vulnérabilités ont été identifiées dans le systèmes d'exploitation Mac OS X. Elles concernent plusieurs applications et services, notamment DHCP, bluetooth, fetchmail, gunzip, ImageIO, telnet, OpenSSH ou LaunchServices. Les risques sont variés, certains peuvant conduire à l'exécution de code arbitraire à distance.

4 Description

De nombreuses vulnérabilités ont été identifiées dans le systèmes d'exploitation Mac OS X. Elles concernent plusieurs applications et services. Parmi celles-ci :

- `DHCP` : le service `bootpd` ne gère pas correctement certaines requêtes, pouvant provoquer un débordement de tampon. Une personne malveillante peut profiter de cette vulnérabilité pour exécuter du code arbitraire à distance, par le biais d'une requête spécialement conçue. Le service `bootpd` n'est cependant pas activé par défaut sur Mac OS X.
- `bluetooth` : la clé secrète générée automatiquement pour la phase d'association avec d'autres appareils bluetooth n'est pas suffisamment longue. Elle facilite les attaques par recherche exhaustive.
- `gunzip` : il serait possible, localement, de modifier les permissions de fichiers appartenant à d'autres utilisateurs exécutant gunzip.
- `ImageIO` : cette application ne gère pas correctement certaines images de type `Radiance` ou `GIF`. L'ouverture d'images malveillantes exploitant ces vulnérabilités peut provoquer un déni de service, ou l'exécution de code arbitraire.
- `OpenSSH` : un utilisateur malveillant peut chercher à se connecter à distance (*remote login*) sur une machine vulnérable en testant plusieurs identifiants. La répétition de cette opération peut conduire à la découverte de comptes valides sur le serveur et à son mauvais fonctionnement (déni de service).
- `telnet` : au cours de la connexion à un serveur Telnet distant, un utilisateur malveillant peut accéder à plusieurs variables d'environnement confidentielles à l'insu de l'utilisateur qui s'y connecte.

D'autres vulnérabilités touchent `dyld` (gestion des liens dynamiques pour les bibliothèques), `AFP Server` (non activé par défaut), `Bom` (système de fichiers pour l'installation), `Image RAW`, `WebKit` et `AppKit`. Les risques sont variés, certains pouvant conduire à l'exécution de code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité 2006-004 Apple du 01 août 2006 :
  http://docs.info.apple.com/article.html?artnum=304063
- Référence CVE CVE-2006-1472 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1472
- Référence CVE CVE-2006-1473 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1473
- Référence CVE CVE-2006-3495 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3495
- Référence CVE CVE-2006-3496 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3496
- Référence CVE CVE-2006-3497 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3497
- Référence CVE CVE-2006-3498 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3498
- Référence CVE CVE-2006-3499 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3499
- Référence CVE CVE-2006-3500 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3500
- Référence CVE CVE-2005-2335 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2335
- Référence CVE CVE-2005-3088 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3088
- Référence CVE CVE-2005-4348 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4348

- Référence CVE CVE-2006-0321 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0321
- Référence CVE CVE-2005-0988 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0988
- Référence CVE CVE-2005-1228 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-1228
- Référence CVE CVE-2006-0392 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0392
- Référence CVE CVE-2006-3501 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3501
- Référence CVE CVE-2006-3502 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3502
- Référence CVE CVE-2006-3503 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3503
- Référence CVE CVE-2006-3504 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3504
- Référence CVE CVE-2006-0393 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0393
- Référence CVE CVE-2005-0393 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0393
- Référence CVE CVE-2005-0488 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0488
- Référence CVE CVE-2006-3505 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3505
- Référence CVE CVE-2006-3459 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3459
- Référence CVE CVE-2006-3461 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3461
- Référence CVE CVE-2006-3462 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3462
- Référence CVE CVE-2006-3465 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3465

Gestion détaillée du document

02 août 2006 version initiale.