Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 novembre 2006
N° CERTA-2006-AVI-517

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Apple Mac OS X

Gestion du document

Référence	CERTA-2006-AVI-517
Titre	Multiples vulnérabilités dans Apple Mac OS X
Date de la première version	29 novembre 2006
Date de la dernière version	–
Source(s)	Bulletin de mises à jour Apple 2006-007 du 28 novembre 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

- Apple Mac OS X v10.3.9 ;
- Apple Mac OS X Server v10.3.9 ;
- Apple Mac OS X v10.4.8 ;
- Apple Mac OS X Server v10.4.8.

3 Résumé

De multiples vulnérabilités ont été identifiées dans le système d'exploitation Apple Mac OS X. Certaines pourraient, si elles sont exploitées par une personne malveillante, provoquer l'exécution de code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été identifiées dans le système d'exploitation Apple Mac OS X. Parmi celles-ci :

- une vulnérabilité des pilotes de cartes sans-fil `Airport` : ils n'interpreteraient pas correctement des paquets répondant à une requête de sondage (de type `Probe`). Une personne malveillante pourrait donc émettre un paquet malformé, en réponse à une requête, afin de provoquer l'exécution de commandes arbitraires à distance. Les solutions de sécurité comme WPA, VPN, 802.11i ne protègent pas de cette catégorie d'attaques visant directement le pilote de la carte réseau. Le CERTA mentionne ce problème dans le bulletin d'actualité CERTA-2006-ACT-046 ;
- une vulnérabilité de `CFNetwork` : les URI (pour *Uniform Resource Identifier*) FTP ne sont pas validées correctement. Une personne pourrait, en visitant un site FTP construit de manière malveillante, lancer à son insu des commandes FTP contre un site tiers ;
- plusieurs vulnérabilités dans `clamAV` pour Mac OS X Server ;
- des vulnérabilités dans OpenSSL pour MacOS. Celles-ci ont été abordées dans des avis du CERTA, notamment CERTA-2006-AVI-421 et CERTA-2006-AVI-448 ;
- des vulnérabilités de `PHP` : certaines ont été décrites dans l'avis du CERTA CERTA-2006-AVI-481 ;
- une vulnérabilité de `PPP` : une personne malveillante pourrait, sur le même réseau qu'une machine vulnérable, envoyer un paquet spécialement conçu, afin de perturber `PPPoE`. Cela permettrait sous certaines conditions d'exécuter des commandes arbitraires à distance. `PPPoE` n'est cependant pas activé par défaut.

5 Solution

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

6 Documentation

- Bulletin de sécurité Apple 2006-007 du 28 novembre 2006 :
  http://docs.info.apple.com/article.html?artnum=304829
- Avis du CERTA CERTA-2006-AVI-421 du 03 octobre 2006 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-421/
- Avis du CERTA CERTA-2006-AVI-448 du 11 octobre 2006 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-448/
- Bulletin d'actualité du CERTA CERTA-2006-ACT-046 du 17 novembre 2006 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-ACT-046.pdf
- Référence CVE CVE-2006-1490 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1490
- Référence CVE CVE-2006-1990 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1990
- Référence CVE CVE-2006-2937 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2937
- Référence CVE CVE-2006-2940 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2940
- Référence CVE CVE-2006-3403 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3403
- Référence CVE CVE-2006-3738 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3738
- Référence CVE CVE-2006-3962 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3962
- Référence CVE CVE-2006-4182 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4182
- Référence CVE CVE-2006-4334 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4334
- Référence CVE CVE-2006-4335 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4335

- Référence CVE CVE-2006-4336 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4336
- Référence CVE CVE-2006-4337 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4337
- Référence CVE CVE-2006-4338 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4338
- Référence CVE CVE-2006-4339 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4339
- Référence CVE CVE-2006-4343 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4343
- Référence CVE CVE-2006-4396 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4396
- Référence CVE CVE-2006-4398 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4398
- Référence CVE CVE-2006-4400 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4400
- Référence CVE CVE-2006-4401 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4401
- Référence CVE CVE-2006-4402 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4402
- Référence CVE CVE-2006-4403 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4403
- Référence CVE CVE-2006-4404 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4404
- Référence CVE CVE-2006-4406 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4406
- Référence CVE CVE-2006-4407 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4407
- Référence CVE CVE-2006-4408 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4408
- Référence CVE CVE-2006-4409 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4409
- Référence CVE CVE-2006-4410 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4410
- Référence CVE CVE-2006-4411 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4411
- Référence CVE CVE-2006-4412 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4412
- Référence CVE CVE-2006-5465 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5465
- Référence CVE CVE-2006-5710 : http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5710

Gestion détaillée du document

29 novembre 2006 version initiale.