Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 août 2005
N° CERTA-2005-AVI-316

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Mac OS X

Gestion du document

Référence	CERTA-2005-AVI-316
Titre	Multiples vulnérabilités dans Mac OS X
Date de la première version	18 août 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité 2005-007 d'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

- Contournement de la politique de sécurité ;
- exécution de code arbitraire ;
- déni de service ;
- élévation de privilèges ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

- Mac OS X 10.4.2 Client et versions antérieures ;
- Mac OS X 10.4.2 Serveur et versions antérieures ;
- Mac OS X 10.3.9 Client et versions antérieures ;
- Mac OS X 10.3.9 Serveur et versions antérieures.

Il est à noter que les versions précédentes de Mac OS X, notamment Jaguar (Mac OS X 10.2), ne font pas l'objet d'un correctif.

3 Résumé

Apple propose un correctif pour Panther (Mac OS X 10.3) et Tiger (Mac OS X 10.4) qui corrige plus de 40 vulnérabilités.

4 Description

De nombreuses vulnérabilités sont corrigées dans la mise à jour de Mac OS X 10.3 et Mac OS X 10.4. Ces vulnérabilités touchent par exemple les services, applications ou bibliothèques suivantes :

- Apache 2 (CAN-2005-1344, CAN-2004-0942, CAN-2004-0885, CAN-2004-1083 et CAN-2004-1084) ;
- AppKit (CAN-2005-2501, CAN-2005-2502 et CAN-2005-2503) ;
- Bluetooth (CAN-2005-2504) ;
- CoreFoundation (CAN-2005-2505 et CAN-2005-2506) ;
- CUPS (CAN-2005-2525 et CAN-2005-2526) ;
- Directory Services (CAN-2005-2507, CAN-2005-2508 et CAN-2005-2519) ;
- HItoolbox (CAN-2005-2513) ;
- Kerberos (CAN-2004-1189, CAN-2005-1174, CAN-2005-1175, CAN-2005-1689 et CAN-2005-2511) ;
- loginwindow (CAN-2005-2509) ;
- Mail (CAN-2005-2512) ;
- MySQL (CAN-2005-0709, CAN-2005-0710 et CAN-2005-0711) ;
- OpenSSL (CAN-2004-0079 et CAN-2004-0112) ;
- ping (CAN-2005-2514) ;
- QuartzComposerScreenSaver (CAN-2005-2515) ;
- Safari (CAN-2005-2516 et CAN-2005-2517) ;
- SecurityInterface (CAN-2005-2520) ;
- servermgrd (CAN-2005-2518) ;
- servermgrd_ipfilter (CAN-2005-2510) ;
- SquirrelMail (CAN-2005-1769 et CAN-2005-2095) ;
- traceroute (CAN-2005-2521) ;
- WebKit (CAN-2005-2522) ;
- Weblog Server (CAN-2005-2523) ;
- X11 (CAN-2005-0605) ;
- zlib (CAN-2005-2096 et CAN-2005-1849).

5 Solution

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

6 Documentation

- Site internet d'apple :
  http://www.apple.com
- Bulletin de sécurité Apple :
  http://docs.info.apple.com/article.html?artnum=302163
- Référence CVE CAN-2005-1344 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1344
- Référence CVE CAN-2004-0942 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0942
- Référence CVE CAN-2004-0885 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0885
- Référence CVE CAN-2004-1083 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1083

- Référence CVE CAN-2004-1084 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1084
- Référence CVE CAN-2005-2501 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2501
- Référence CVE CAN-2005-2502 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2502
- Référence CVE CAN-2005-2503 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2503
- Référence CVE CAN-2005-2504 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2504
- Référence CVE CAN-2005-2505 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2505
- Référence CVE CAN-2005-2506 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2506
- Référence CVE CAN-2005-2525 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2525
- Référence CVE CAN-2005-2526 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2526
- Référence CVE CAN-2005-2507 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2507
- Référence CVE CAN-2005-2508 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2508
- Référence CVE CAN-2005-2519 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2519
- Référence CVE CAN-2005-2513 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2513
- Référence CVE CAN-2004-1189 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1189
- Référence CVE CAN-2005-1174 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1174
- Référence CVE CAN-2005-1175 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1175
- Référence CVE CAN-2005-1689 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1689
- Référence CVE CAN-2005-2511 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2511
- Référence CVE CAN-2005-2509 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2509
- Référence CVE CAN-2005-2512 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2512
- Référence CVE CAN-2005-0709 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0709
- Référence CVE CAN-2005-0710 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0710
- Référence CVE CAN-2005-0711 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0711
- Référence CVE CAN-2004-0079 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0079
- Référence CVE CAN-2004-0112 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0112
- Référence CVE CAN-2005-2514 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2514

- Référence CVE CAN-2005-2515 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2515
- Référence CVE CAN-2005-2516 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2516
- Référence CVE CAN-2005-2517 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2517
- Référence CVE CAN-2005-2520 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2520
- Référence CVE CAN-2005-2518 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2518
- Référence CVE CAN-2005-2510 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2510
- Référence CVE CAN-2005-1769 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1769
- Référence CVE CAN-2005-2095 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2095
- Référence CVE CAN-2005-2521 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2521
- Référence CVE CAN-2005-2522 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2522
- Référence CVE CAN-2005-2523 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2523
- Référence CVE CAN-2005-0605 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0605
- Référence CVE CAN-2005-2096 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2096
- Référence CVE CAN-2005-1849 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1849

Gestion détaillée du document

18 août 2005 version initiale.