

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Mutiples vulnérabilités dans Apple Mac OS X

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-278>

Gestion du document

Référence	CERTA-2008-AVI-278
Titre	Mutiples vulnérabilités dans Apple Mac OS X
Date de la première version	29 mai 2008
Date de la dernière version	–
Source(s)	Mises à jour de sécurité Apple 2008-003 du 28 mai 2008
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 v10.5.x ;
- Apple Mac OS X versions v10.4.x.

3 Résumé

Plusieurs vulnérabilités concernant le système d'exploitation Apple Mac OS X ont été identifiées. L'exploitation de ces dernières peut avoir plusieurs conséquences, dont des exécutions de codes arbitraires à distance.

4 Description

Plusieurs vulnérabilités concernant le système d'exploitation Apple Mac OS X ont été identifiées :

- le serveur AFP (*Apple Filing Protocol*) ne vérifie pas correctement la cohérence d'accès entre répertoires et fichiers.
- le serveur Apache est mis à jour en 2.0.63 pour les versions Mac OS X Server v10.4.x ; nouvelle version qui corrige des vulnérabilités permettant des attaques par injection de code indirecte ;
- l'impression d'un document PDF spécialement construit par ATS peut provoquer l'exécution de code arbitraire ;
- l'impression de documents via CUPS à destination d'une imprimante peut permettre sous certaines conditions de récupérer des informations sensibles, y compris si une protection par mot de passe est déployée ;
- des vulnérabilités dans le module Flash Player sont corrigées (cf. CERTA-2008-AVI-197) ;
- les vulnérabilités détaillées dans l'alerte CERTA-2008-ALE-007 concernant iCal sont corrigées ;
- etc.

5 Solution

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

6 Documentation

- Alerte CERTA-2008-ALE-007, « Multiples vulnérabilités dans Apple Ical », du 23 mai 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-007/>
- Bulletin de sécurité Apple 106704 du 28 mai 2008 :
<http://docs.info.apple.com/article.html?artnum=106704>
- Détails de la mise à jour de sécurité 2008-003 / Mac OS X 10.5.3 :
<http://support.apple.com/kb/HT1897>
- Tableau récapitulatif des mises à jour de sécurité pour Mac OS X :
http://support.apple.com/kb/HT1222?viewlocale=fr_FR
- Référence CVE CVE-2005-3352 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3352>
- Référence CVE CVE-2005-3357 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3357>
- Référence CVE CVE-2006-3747 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3747>
- Référence CVE CVE-2007-0071 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0071>
- Référence CVE CVE-2007-1863 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1863>
- Référence CVE CVE-2007-3847 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3847>
- Référence CVE CVE-2007-4465 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4465>
- Référence CVE CVE-2007-5000 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5000>
- Référence CVE CVE-2007-5267 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5267>
- Référence CVE CVE-2007-5268 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5268>
- Référence CVE CVE-2007-5268 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5268>
- Référence CVE CVE-2007-5269 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5269>

- Référence CVE CVE-2007-5275 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5275>
- Référence CVE CVE-2007-6019 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6019>
- Référence CVE CVE-2007-6243 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6243>
- Référence CVE CVE-2007-6359 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6359>
- Référence CVE CVE-2007-6388 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6388>
- Référence CVE CVE-2007-6612 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6612>
- Référence CVE CVE-2008-0177 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0177>
- Référence CVE CVE-2008-1027 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1027>
- Référence CVE CVE-2008-1028 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1028>
- Référence CVE CVE-2008-1030 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1030>
- Référence CVE CVE-2008-1031 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1031>
- Référence CVE CVE-2008-1032 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1032>
- Référence CVE CVE-2008-1033 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1033>
- Référence CVE CVE-2008-1034 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1034>
- Référence CVE CVE-2008-1035 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1035>
- Référence CVE CVE-2008-1036 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1036>
- Référence CVE CVE-2008-1571 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1571>
- Référence CVE CVE-2008-1572 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1572>
- Référence CVE CVE-2008-1573 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1573>
- Référence CVE CVE-2008-1574 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1574>
- Référence CVE CVE-2008-1575 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1575>
- Référence CVE CVE-2008-1576 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1576>
- Référence CVE CVE-2008-1577 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1577>
- Référence CVE CVE-2008-1578 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1578>
- Référence CVE CVE-2008-1579 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1579>
- Référence CVE CVE-2008-1580 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1580>

- Référence CVE CVE-2008-1654 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1654>
- Référence CVE CVE-2008-1655 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1655>

Gestion détaillée du document

29 mai 2008 version initiale.