

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2005-AVI-034>

Gestion du document

Référence	CERTA-2005-AVI-034-001
Titre	Multiples vulnérabilités dans Mac OS X
Date de la première version	27 janvier 2005
Date de la dernière version	23 juin 2005
Source(s)	Bulletin de sécurité d'Apple du 21 janvier 2005
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

- Elévation de privilèges ;
- déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Mac OS X v10.2.8 ;
- Mac OS X v10.3.7 ;
- Mac OS X Server v10.2.8 ;
- Mac OS X Server v10.3.7.

3 Résumé

De multiples vulnérabilités découvertes dans le système d'exploitation Mac OS X d'Apple peuvent être exploitées par un utilisateur mal intentionné afin de réaliser un déni de service, d'exécuter du code arbitraire à distance, ou d'élever ses privilèges.

4 Description

- Une vulnérabilité affecte les commandes de la famille `at`, permettant d'élever les privilèges (référence CVE CAN-2005-0125). La mise à jour concerne les commandes `at`, `atrm`, `batch`, `atq`, et `atrun` ;
- une vulnérabilité affecte le composant `ColorSync`. Un utilisateur mal intentionné peut, par le biais de profils de couleur ICC mal formés, exécuter du code arbitraire (référence CVE CAN-2005-0126) ;
- une vulnérabilité décrite dans l'avis CERTA-2004-AVI-361 affecte la bibliothèque `libxml2` (référence CVE CAN-2004-0989) ;
- une vulnérabilité affecte le composant `Mail`. Des informations relatives à la carte réseau sont ajoutées dans l'en-tête des messages (référence CVE CAN-2005-0127) ;
- de multiples vulnérabilités décrites dans l'avis CERTA-2004-AVI-405 affectent le composant `PHP`. L'exploitation de ces vulnérabilités permet de réaliser un déni de service ou l'exécution de code arbitraire à distance (référence CVE CAN-2003-0860, CAN-2003-0863, CAN-2004-0594, CAN-2004-0595, CAN-2004-1018, CAN-2004-1019, CAN-2004-1020, CAN-2004-1063, CAN-2004-1064, CAN-2004-1065). L'application du correctif d'Apple met à jour `PHP` en version 4.3.10 ;
- une vulnérabilité affecte le navigateur `Safari`. Si la fonctionnalité de blocage des fenêtres `pop-up` n'est pas activée, un utilisateur peut être trompé sur le contenu d'une telle fenêtre (référence CVE CAN-2004-1314) ;
- une vulnérabilité de type `cross-site scripting` affecte `SquirrelMail` (référence CVE CAN-2004-1036).

5 Solution

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

6 Documentation

- Bulletin de sécurité d'Apple du 21 janvier 2005 :
<http://docs.info.apple.com/article.html?artnum=300770>
- Bulletin de sécurité CERTA-2004-AVI-361 du CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-361>
- Bulletin de sécurité CERTA-2004-AVI-405 du CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-405>
- Référence CVE CAN-2003-0860 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0860>
- Référence CVE CAN-2003-0863 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0863>
- Référence CVE CAN-2004-0594 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0594>
- Référence CVE CAN-2004-0595 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0595>
- Bulletin de sécurité SGI #20050602-01-U du 09 juin 2005 (CVE CAN-2004-0989) :
<ftp://patches.sgi.com/support/free/security/advisories/20050602-01-U.asc>
- Référence CVE CAN-2004-0989 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0989>
- Référence CVE CAN-2004-1018 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1018>
- Référence CVE CAN-2004-1019 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1019>
- Référence CVE CAN-2004-1020 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1020>
- Référence CVE CAN-2004-1036 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1036>
- Référence CVE CAN-2004-1063 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1063>

- Référence CVE CAN-2004-1064 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1064>
- Référence CVE CAN-2004-1065 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1065>
- Référence CVE CAN-2004-1314 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1314>
- Référence CVE CAN-2005-0125 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0125>
- Référence CVE CAN-2005-0126 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0126>
- Référence CVE CAN-2005-0127 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0127>

Gestion détaillée du document

27 janvier 2005 version initiale.

23 juin 2005 ajout de la référence au bulletin de sécurité SGI