

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de Apple MacOS 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-2006-AVI-262>

Gestion du document

Référence	CERTA-2006-AVI-262
Titre	Vulnérabilités de Apple MacOS X
Date de la première version	29 juin 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple du 27 juin 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 ;
- élévation de privilèges ;
- déni de service ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

MacOS X 10.4 jusqu'à la version 10.4.6.

3 Résumé

De multiples vulnérabilités dans Apple MacOS X permettent à un utilisateur mal intentionné de porter atteinte à la confidentialité des données, de réaliser un déni de service ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

4 Description

De multiples vulnérabilités affectent Apple MacOS X :

- Une vulnérabilité dans le serveur AFP (Apple File Protocol) permet à un utilisateur mal intentionné de porter atteinte à la confidentialité des données (CVE-2006-1468) ;
- une vulnérabilité dans ClamAV permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance (CVE-2006-1989) ;
- une vulnérabilité dans ImageIO permet à un utilisateur mal intentionné d'exécuter du code arbitraire au moyen d'un fichier image au format TIFF habilement constitué (CVE-2006-1469) ;
- une vulnérabilité dans launchd permet à un utilisateur local authentifié d'élèver ses privilèges (CVE-2006-1471) ;
- une vulnérabilité dans OpenLDAP permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance au moyen d'une requête LDAP habilement constituée (CVE-2006-1470).

5 Solution

Mettre à jour Apple MacOS X en version 10.4.7. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple du 27 juin 2006 :
<http://docs.info.apple.com/article.html?artnum=303973>
- Référence CVE CVE-2006-1468 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1468>
- Référence CVE CVE-2006-1469 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1469>
- Référence CVE CVE-2006-1470 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1470>
- Référence CVE CVE-2006-1471 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1471>
- Référence CVE CVE-2006-1989 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1989>

Gestion détaillée du document

29 juin 2006 version initiale.