



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 26 mai 2005  
N° CERTA-2005-AVI-177

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-177>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2005-AVI-177                     |
| Titre                       | Multiples vulnérabilités dans Mac OS X |
| Date de la première version | 26 mai 2005                            |
| Date de la dernière version | –                                      |
| Source(s)                   | Bulletin de sécurité 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 sécurité ;
- diffusion d'informations sensibles ;
- déni de service.

## 2 Systèmes affectés

Apple Mac OS X versions antérieures à la version 10.4.1.

## 3 Résumé

De multiples vulnérabilités sont présentes sur le système d'exploitation Mac OS X. Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné pour réaliser un déni de service ou contourner la sécurité sur le système vulnérable.

## 4 Description

Cinq vulnérabilités sont présentes sur le système d'exploitation Mac OS X :

- La première vulnérabilité est exploitable sur un système où l'utilisation du Bluetooth est activée. Cette vulnérabilité permet à un utilisateur mal intentionné de réaliser une traversée d'arborecence sur le système vulnérable ;
- une vulnérabilité liée au navigateur Safari peut être exploitée via un site Internet malicieusement construit pour télécharger et installer un programme malicieux sur le système ;
- une vulnérabilité dans deux appels système peut être exploitée par un utilisateur mal intentionné pour obtenir le nom d'un fichier dans un répertoire caché ;
- une vulnérabilité dans la fonction `nfs_mount` peut être utilisée pour réaliser un déni de service ;
- une dernière vulnérabilité peut être exploitée par un utilisateur ayant un accès physique à la machine pour démarrer des applications sur une machine ayant l'économiseur d'écran verrouillé.

## 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=301630>
- Référence CVE CAN-2005-0974 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0974>
- Référence CVE CAN-2005-1333 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1333>
- Référence CVE CAN-2005-1472 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1472>
- Référence CVE CAN-2005-1473 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1474>
- Référence CVE CAN-2005-1474 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1474>

## Gestion détaillée du document

26 mai 2005 version initiale.