

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-2004-AVI-309>

---

### Gestion du document

Référence	CERTA-2004-AVI-309
Titre	Multiples vulnérabilités dans Mac OS X
Date de la première version	09 septembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple du 07 Septembre 2004
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 ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données.

## 2 Systèmes affectés

- Mac OS X versions 10.2.8, 10.3.4 et 10.3.5 ;
- Mac OS X Server versions 10.2.8, 10.3.4 et 10.3.5.

## 3 Résumé

De nombreuses vulnérabilités sont présentes dans Mac OS X et Mac OS X Server permettant d'exécuter du code arbitraire à distance, d'effectuer des dénis de service ou de porter atteinte à la confidentialité et à l'intégrité des données.

## 4 Description

Plusieurs vulnérabilités sont présentes dans Mac OS X. Certaines de ces vulnérabilités ont déjà fait l'objet d'un avis du CERTA :

- Une vulnérabilité est présente dans Apache 2 permettant à un individu mal intentionné d'effectuer un déni de service sur le serveur affecté (cf. avis CERTA-2004-AVI-210 du CERTA, références CVE CAN-2004-0493 et CAN-2004-0488) ;
- deux vulnérabilités dans le composant CoreFoundation permettent à un utilisateur local mal intentionné d'exécuter du code arbitraire et d'élever ses privilèges (vulnérabilités CAN-2004-0821 et CAN-2004-0822) ;
- une vulnérabilité dans IPSec permet à un individu mal intentionné de contourner certaines restrictions de sécurité (cf. avis CERTA-2004-AVI-259 du CERTA et référence CVE CAN-2004-0607) ;
- une vulnérabilité dans Kerberos permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance (cf. avis CERTA-2004-AVI-286 du CERTA et référence CVE CAN-2004-0523) ;
- une vulnérabilité du service FTP du logiciel lukemftpd permet à un utilisateur mal intentionné préalablement authentifié d'exécuter du code arbitraire à distance ou d'effectuer un déni de service (cf. avis CERTA-2004-AVI-272 du CERTA et référence CVE CAN-2004-794) ;
- une vulnérabilité dans la gestion des mots de passe de l'annuaire OpenLDAP (vulnérabilité CAN-2004-0823) ;
- une vulnérabilité dans l'utilitaire SCP d'OpenSSH permet de porter atteinte à l'intégrité des données (cf. avis CERTA-2004-AVI-308 du CERTA et référence CVE CAN-2004-0175) ;
- une vulnérabilité dans PPPDialer permet à un utilisateur mal intentionné d'écraser des fichiers arbitraires présents sur le système affecté afin d'élever ses privilèges (vulnérabilité CAN-2004-0824) ;
- une vulnérabilité présente dans le serveur de streaming QuickTime permet à un utilisateur mal intentionné d'effectuer un déni de service (vulnérabilité CAN-2004-0825) ;
- une vulnérabilité dans l'application de copie de fichiers rsync permet à un utilisateur mal intentionné d'accéder à des fichiers situés en dehors du répertoire de base (cf. avis CERTA-2004-AVI-271 du CERTA et référence CVE CAN-2004-0426) ;
- deux vulnérabilités présentes dans le navigateur Safari permet à un individu mal intentionné de substituer l'identité réelle d'un site (vulnérabilité CAN-2004-0361) et d'injecter du code arbitraire à distance (vulnérabilité CAN-2004-0720) ;
- une vulnérabilité dans le webmail SquirrelMail permet à un individu mal intentionné d'exécuter une requête SQL non sollicitée (cf. avis CERTA-2004-AVI-263 du CERTA et référence CVE CAN-2004-0521) ;
- une vulnérabilité dans l'application réseau TCPDUMP permet à un utilisateur mal intentionné d'effectuer un arrêt brutal de TCPDUMP par l'envoi de paquets malicieux (cf. avis CERTA-2004-AVI-106 du CERTA et référence CVE CAN-2004-0183 et CAN-2004-0184).

## 5 Solution

Appliquer le correctif fournit par l'éditeur suivant la version affectée :

- Mac OS X 10.2.8 :  
[http://www.apple.com/support/downloads/securityupdate\\_2004-09-07\\_\(10\\_2\\_8\\_Client\).html](http://www.apple.com/support/downloads/securityupdate_2004-09-07_(10_2_8_Client).html)
- Mac OS X Server 10.2.8 :  
[http://www.apple.com/support/downloads/securityupdate\\_2004-09-07\\_\(10\\_2\\_8\\_Server\).html](http://www.apple.com/support/downloads/securityupdate_2004-09-07_(10_2_8_Server).html)
- Mac OS X 10.3.4 :  
[http://www.apple.com/support/downloads/securityupdate\\_2004-09-07\\_\(10\\_3\\_4\\_Client\).html](http://www.apple.com/support/downloads/securityupdate_2004-09-07_(10_3_4_Client).html)
- Mac OS X Server 10.3.4 :  
[http://www.apple.com/support/downloads/securityupdate\\_2004-09-07\\_\(10\\_3\\_4\\_Server\).html](http://www.apple.com/support/downloads/securityupdate_2004-09-07_(10_3_4_Server).html)
- Mac OS X 10.3.5 :  
[http://www.apple.com/support/downloads/securityupdate\\_2004-09-07\\_\(10\\_3\\_5\\_Client\).html](http://www.apple.com/support/downloads/securityupdate_2004-09-07_(10_3_5_Client).html)
- Mac OS X Server 10.3.5 :  
[http://www.apple.com/support/downloads/securityupdate\\_2004-09-07\\_\(10\\_3\\_5\\_Server\).html](http://www.apple.com/support/downloads/securityupdate_2004-09-07_(10_3_5_Server).html)

## 6 Documentation

- Bulletin de sécurité Apple du 07 Septembre 2004 :  
<http://docs.info.apple.com/article.html?artnum=61798>
- Bulletin de sécurité CERTA-2004-AVI-210 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-210/>
- Bulletin de sécurité CERTA-2004-AVI-286 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-286/>
- Bulletin de sécurité CERTA-2004-AVI-308 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-308/>
- Bulletin de sécurité CERTA-2004-AVI-271 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-271/>
- Bulletin de sécurité CERTA-2004-AVI-263 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-263/>
- Bulletin de sécurité CERTA-2004-AVI-106 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2004-AVI-106/>
- Référence CVE CAN-2004-0821 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0821>
- Référence CVE CAN-2004-0822 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0822>
- Référence CVE CAN-2004-0823 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0823>
- Référence CVE CAN-2004-0824 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0824>
- Référence CVE CAN-2004-0825 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0825>

### Gestion détaillée du document

**09 septembre 2004** version initiale.