

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités sous 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-018>

---

### Gestion du document

Référence	CERTA-2004-AVI-018
Titre	Multiples vulnérabilités sous Mac OS X
Date de la première version	29 janvier 2004
Date de la dernière version	–
Source(s)	Mise-à-jour de sécurité 2004-01-26 d'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

- Elévation de privilèges ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données.

## 2 Systèmes affectés

- Mac OS X 10.1.5 (CAN-2004-085) ;
- Mac OS X 10.2.8 (CAN-2004-085, CAN-2004-087, CAN-2004-088, CAN-2004-089, CAN-2004-092, CAN-2003-0542, CAN-2003-0789) ;
- Mac OS X 10.3.2 (CAN-2004-086, CAN-2004-087, CAN-2004-089, CAN-2004-090, CAN-2003-0542, CAN-2003-0789).

## 3 Description

Apple a émis un bulletin concernant une mise à jour des différentes versions de Mac OS X. Cette mise à jour est relative à des failles de sécurité présentes dans plusieurs composants de Mac OS X :

- serveur HTTP Apache : CAN-2003-0542, CAN-2003-0789 ;

- client de messagerie Apple Mail : CAN-2004-085 et CAN-2004-086 ;
- navigateur Safari : CAN-2004-092 ;
- outil de configuration système : CAN-2004-087, CAN-2004-088 ;
- émulateur MacOS Classic : CAN-2004-089 ;
- partage de fichiers Windows : CAN-2004-090.

Les vulnérabilités CAN-2003-0542 et CAN-2003-0789 sont décrites dans le bulletin de sécurité CERTA-2003-AVI-177 du CERTA.

La vulnérabilité CAN-2004-089 est une vulnérabilité de type débordement de mémoire présente dans l'exécutable `TruBlueEnvironment`. Cette vulnérabilité peut être exploitée par un utilisateur local mal intentionné afin de réaliser une élévation de privilèges sur la plate-forme vulnérable.

## 4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs :

<http://docs.info.apple.com/article.html?artnum=61798>

## 5 Documentation

- Bulletin de sécurité "TruBlueEnvironment Buffer Overflow" d'Atstake :  
<http://www.atstake.com/research/advisories/2004/a012704-1.txt>
- Bulletin de sécurité CERTA-2003-AVI-177 du CERTA :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-177/index.html>
- Référence CVE CAN-2004-085 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0085>
- Référence CVE CAN-2004-086 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0086>
- Référence CVE CAN-2004-087 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0087>
- Référence CVE CAN-2004-088 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0088>
- Référence CVE CAN-2004-089 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0089>
- Référence CVE CAN-2004-090 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0090>
- Référence CVE CAN-2004-092 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0092>

## Gestion détaillée du document

29 janvier 2004 version initiale.