



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 18 mai 2004  
N° CERTA-2004-AVI-086-003

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du serveur HTTP Apache

---

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-086>

---

### Gestion du document

Référence	CERTA-2004-AVI-086-003
Titre	Vulnérabilité du serveur HTTP Apache
Date de la première version	15 mars 2004
Date de la dernière version	18 mai 2004
Source(s)	Avis OpenBSD #014 du 13 mars 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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

Serveur HTTP Apache 1.3.x sur les plates-formes 64 bits *big endian*.

## 3 Résumé

Une vulnérabilité du serveur HTTP Apache permet à un utilisateur mal intentionné de contourner la politique de sécurité.

## 4 Description

Le module *mod\_access* du serveur HTTP Apache présente une vulnérabilité dans le traitement des règles *Allow/Deny* qui utilisent des adresses IP sans masque de réseau.

Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné pour contourner des règles de sécurité.

## 5 Solution

Appliquer le correctif fournit par votre éditeur.

La version 1.3.30 d'Apache corrigera cette vulnérabilité. En attendant la sortie de cette version, appliquer le correctif disponible à l'adresse suivante :

[http://cvs.apache.org/viewcvs.cgi/apache-1.3/src/modules/standard/mod\\_access.c?r1=1.46&r2=1.47](http://cvs.apache.org/viewcvs.cgi/apache-1.3/src/modules/standard/mod_access.c?r1=1.46&r2=1.47)

## 6 Documentation

- Bug du serveur HTTP Apache #23850 :  
[http://nagoya.apache.org/bugzilla/show\\_bug.cgi?id=23850](http://nagoya.apache.org/bugzilla/show_bug.cgi?id=23850)
- Avis de sécurité Mandrake MDKSA-2004:046 :  
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:046>
- Avis de sécurité OpenBSD #014 du 13 mars 2004 :  
<http://www.openbsd.org/errata.html>
- Avis de sécurité FreeBSD du 08 mars 2004 :  
<http://www.vuxml.org/freebsd/>
- Référence CVE CAN-2003-0993 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0993>

## Gestion détaillée du document

**15 mars 2004** version initiale.

**16 mars 2004** correction du lien sur le correctif.

**12 mai 2004** ajout de la référence au bulletin de sécurité FreeBSD.

**18 mai 2004** ajout de la référence à l'avis Mandrake.