



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 08 septembre 2004  
N° CERTA-2004-AVI-210-006

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-210>

---

### Gestion du document

Référence	CERTA-2004-AVI-210-006
Titre	Vulnérabilité du serveur HTTP Apache
Date de la première version	29 juin 2004
Date de la dernière version	08 septembre 2004
Source(s)	Avis de sécurité de Guninski #70
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

Déni de service.

## 2 Systèmes affectés

Serveur HTTP Apache version 2.0.49 et versions antérieures.

## 3 Résumé

Une vulnérabilité du serveur HTTP Apache permet à un utilisateur mal intentionné de provoquer un déni de service sur le serveur vulnérable.

## 4 Description

Une mauvaise gestion des en-têtes par le serveur HTTP Apache (série 2.0 uniquement) permet à un utilisateur mal intentionné de saturer la mémoire du serveur vulnérable.

## 5 Solution

La version 2.0.50-dev du serveur HTTP Apache corrige cette vulnérabilité.

## 6 Documentation

- Site Internet du serveur HTTP Apache :  
<http://httpd.apache.org>
- Avis de sécurité de Georgi Guninski #70 du 28 juin 2004 :  
<http://www.guninski.com/httpd1.html>
- Article sur le site de nouvelles du serveur HTTP Apache :  
<http://www.apacheweek.com/features/security-20>
- Bulletin de sécurité Mandrake MDKSA-2004:064 du 29 juin 2004 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:064>
- Bulletin de sécurité Gentoo GLSA 200407-03 du 04 juillet 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200407-03.xml>
- Bulletin de sécurité RedHat RHSA-2004:342 du 06 juillet 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-342.html>
- Bulletin de sécurité IBM pour IBM HTTP Server :  
<http://www-1.ibm.com/support/docview.wss?rs=177&context=SSEQTJ&uid=swg21174271>
- Bulletin de sécurité HP HPSBUX01064 du 02 août 2004 :  
<http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX01064>
- Bulletin de sécurité Apple du 07 septembre 2004 :  
<http://docs.info.apple.com/article.html?artnum=61798>
- Référence CVE CAN-2004-0493 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0493>

## Gestion détaillée du document

**29 juin 2004** version initiale.

**30 juin 2004** ajout de la référence au bulletin de sécurité Mandrake.

**05 juillet 2004** ajout de la référence au bulletin de sécurité Gentoo.

**06 juillet 2004** ajout de la référence au bulletin de sécurité RedHat.

**29 juillet 2004** ajout de la référence au bulletin de sécurité IBM.

**07 août 2004** ajout de la référence au bulletin de sécurité HP.

**08 septembre 2004** ajout de la référence au bulletin de sécurité Apple.