



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 12 mai 2004  
N° CERTA-2004-AVI-079-008

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-079>

---

### Gestion du document

Référence	CERTA-2004-AVI-079-008
Titre	Vulnérabilité du serveur HTTP Apache
Date de la première version	11 mars 2004
Date de la dernière version	12 mai 2004
Source(s)	Bug Apache #27106
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 versions 2.0.35 à 2.0.48 avec le module *mod\_ssl* activé.

## 3 Résumé

Un utilisateur mal intentionné peut provoquer un déni de service sur un serveur HTTP Apache dont le module *mod\_ssl* est activé.

## 4 Description

Une mauvaise gestion de la mémoire dans le module *mod\_ssl* permet à un utilisateur mal intentionné de provoquer l'arrêt brutal du serveur HTTP Apache.

Cette vulnérabilité peut être exploitée en envoyant des paquets *HTTP* sur le port du serveur *HTTPS* (le port par défaut est le 443/tcp).

## 5 Contournement provisoire

Désactiver le module *mod\_ssl* si ce dernier n'est pas nécessaire.

Filtrer le port 443/tcp sur les pare-feux pour limiter les attaques venant de l'extérieur.

## 6 Solution

La version 2.0.49 corrige cette vulnérabilité.

Pour les versions actuelles, appliquer le correctif disponible à l'adresse suivante :

[http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl\\_engine\\_io.c?r1=1.100.2.11&r2=1.100.2.12](http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.100.2.11&r2=1.100.2.12)

## 7 Documentation

Correctifs intégrés à la version 2.0.49 d'Apache :

[http://www.apache.org/dist/httpd/CHANGES\\_2.0](http://www.apache.org/dist/httpd/CHANGES_2.0)

Bug du serveur HTTP Apache #27106 :

[http://nagoya.apache.org/bugzilla/show\\_bug.cgi?id=27106](http://nagoya.apache.org/bugzilla/show_bug.cgi?id=27106)

Avis de sécurité RedHat RHSA-2004:084-14 pour Red Hat Enterprise Linux :

<http://rhn.redhat.com/errata/RHSA-2004-084.html>

Avis de sécurité RedHat RHSA-2004:182 pour Red Hat Linux :

<http://rhn.redhat.com/errata/RHSA-2004-182.html>

Avis de sécurité GLSA 200403-04 :

<http://www.securityfocus.com/advisories/6472>

Bulletin de sécurité HPSBUX01022 pour HP-UX :

<http://www.securityfocus.com/advisories/6621>

Bulletin de sécurité MDKSA-2004:043 de Mandrake :

<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:043>

Avis de sécurité FreeBSD du 08 mars 2004 :

<http://www.vuxml.org/freebsd/>

Mise à jour de sécurité du paquetage NetBSD apache2 :

<ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities>

Référence CVE CAN-2004-0113 :

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0113>

## Gestion détaillée du document

**11 mars 2004** version initiale.

**16 mars 2004** première révision : correction dans le lien du correctif.

**22 mars 2004** sortie de la version 2.0.49 : ajout référence dans la section Documentation.

**24 mars 2004** troisième révision : ajout de l'avis RedHat.

**29 mars 2004** Ajout référence au bulletin de sécurité de Gentoo.

**27 avril 2004** Ajout référence au bulletin de Hewlett-Packard.

**30 avril 2004** Ajout référence au bulletin RHSA-2004:182 pour red Hat Linux.

**12 mai 2004** Ajout référence au bulletin de sécurité de Mandrake.

**12 mai 2004** Ajout références aux bulletins de sécurité FreeBSD et NetBSD.