

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du module mod\_ssl dans Apache 2

---

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-2006-AVI-013>

---

### Gestion du document

Référence	CERTA-2006-AVI-013-001
Titre	Vulnérabilité du module mod_ssl dans Apache 2
Date de la première version	10 janvier 2006
Date de la dernière version	27 février 2006
Source(s)	Bugzilla d'Apache numero 37791
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 à distance.

## 2 Systèmes affectés

- Apache version 2.0.55 et versions antérieures ;
- Apache version 2.2.0 et versions antérieures ;
- Apache version 2.1.10 et versions antérieures.

## 3 Résumé

Une vulnérabilité dans le module mod\_ssl d'apache permet à un utilisateur mal intentionné de réaliser un déni de service à distance.

## 4 Description

Une vulnérabilité a été découverte dans le module mod\_ssl du serveur web Apache 2.

Un utilisateur mal intentionné peut exploiter cette vulnérabilité par l'intermédiaire d'une requête normale (c'est à dire non SSL) spécialement construite, à destination d'un hôte virtuel SSL.

Cette vulnérabilité n'est exploitable que dans le cas où l'hôte virtuel a été configuré pour fournir une page d'erreur particulière comme réponse aux erreurs de type 400.

## 5 Solution

Une mise à jour est disponible sur le CVS d'Apache :  
[http://issues.apache.org/bugzilla/show\\_bug.cgi?id=37791](http://issues.apache.org/bugzilla/show_bug.cgi?id=37791)

## 6 Documentation

- Site de l'éditeur :  
<http://www.apache.org>
- Report de ce bug sur le site d'Apache :  
[http://issues.apache.org/bugzilla/show\\_bug.cgi?id=37791](http://issues.apache.org/bugzilla/show_bug.cgi?id=37791)
- Bulletin de sécurité Mandriva MDSKA-2006:007 du 05 janvier 2006 :  
<http://wwwnew.mandriva.com/security/advisories?name=MDSKA-2006:007>
- Bulletin de sécurité RedHat RHSA-2006:00159 du 06 janvier 2006 :  
<http://rhn.redhat.com/errata/RHSA-2006-00159.html>
- Bulletin de sécurité SUSE SUSE-SR:2006:004 du 24 février 2006 :  
[http://www.novell.com/linux/security/advisories/2006\\_04\\_sr.html](http://www.novell.com/linux/security/advisories/2006_04_sr.html)
- Référence CVE CVE-2005-3357 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3357>

## Gestion détaillée du document

**10 janvier 2006** version initiale.

**27 février 2006** ajout de la référence au bulletin de sécurité SUSE.