

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans mod\_ssl

---

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-2005-AVI-331>

---

### Gestion du document

Référence	CERTA-2005-AVI-331-001
Titre	Vulnérabilité dans mod_ssl
Date de la première version	05 septembre 2005
Date de la dernière version	19 septembre 2005
Source(s)	Site Internet de mod_ssl
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 des règles de sécurité.

## 2 Systèmes affectés

mod\_ssl versions 2.x antérieures à la version 2.8.4.

## 3 Description

mod\_ssl est un module pour le serveur web apache destiné à assurer les fonctions de cryptographie de ce serveur.

Une vulnérabilité présente sur ce module permet à un utilisateur mal intentionné d'accéder à des pages Internet non autorisées. Cette vulnérabilité est due à un problème dans la vérification des certificats client.

## 4 Contournement provisoire

Mettre à jour le module avec la version 2.8.24.

## 5 Solution

- Site Internet de mod\_ssl :  
<http://www.modssl.org/>
- Mise à jour de mod\_ssl :  
[http://www.modssl.org/source/mod\\_ssl-2.8.24-1.3.33.tar.gz](http://www.modssl.org/source/mod_ssl-2.8.24-1.3.33.tar.gz)
- Bulletin de sécurité SUSE SuSE-SA:2005:051 du 12 septembre 2005 :  
[http://www.novell.com/linux/security/advisories/2005\\_51\\_apache2.html](http://www.novell.com/linux/security/advisories/2005_51_apache2.html)
- Debian Linux :
  - Bulletin de sécurité Debian DSA-805 du 08 septembre 2005 (apache2) :  
<http://www.debian.org/security/2005/dsa-805>
  - Bulletin de sécurité Debian DSA-807 du 12 septembre 2005 (libapache-mod-ssl) :  
<http://www.debian.org/security/2005/dsa-807>
- Bulletin de sécurité Mandriva MDKSA-2005:161 du 08 septembre 2005 :  
<http://www.mandriva.com/security/advisories?name=MDKSA-2005:161>
- Bulletins de sécurité Red Hat Linux RHSA-2005-773 du 15 septembre 2005 :  
<http://rhn.redhat.com/errata/RHSA-2005-773.html>
- Bulletin de sécurité Gentoo GLSA-200509-12 du 19 septembre 2005 :  
<http://www.gentoo.org/security/en/glsa/glsa-200509-12.xml>
- Référence CVE CAN-2005-2700 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2700>

## 6 Documentation

### Gestion détaillée du document

**05 septembre 2005** version initiale :

**19 septembre 2005** ajout des bulletins de sécurité SuSE, RedHat, Mandriva, Gentoo, Debian et de la référence CVE.