

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du module Apache 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-2004-AVI-178>

---

### Gestion du document

Référence	CERTA-2004-AVI-178-006
Titre	Vulnérabilité du module Apache mod_ssl
Date de la première version	02 juin 2004
Date de la dernière version	08 septembre 2004
Source(s)	Avis SA11534 de Secunia Bulletin de sécurité MDKSA-2004:054 de Mandrake Bulletin de sécurité MDKSA-2004:055 de Mandrake
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

- Exécution de code arbitraire à distance ;
- déni de service.

## 2 Systèmes affectés

- mod\_ssl versions antérieures à 2.8.18.
- Apache 2.0.x.

## 3 Résumé

Une vulnérabilité présente dans le module mod\_ssl d'Apache peut être exploitée par un utilisateur mal intentionné pour réaliser, sous certaines conditions, l'exécution de code arbitraire à distance ou provoquer un déni de service.

## 4 Description

Une vulnérabilité de type débordement de mémoire est présente dans la fonction `ssl_util_uencode_binary()` du module `mod_ssl` d'Apache, fonction appelée lors de la vérification des certificats client.

Par le biais d'un certificat habilement constitué, un utilisateur mal intentionné peut exécuter du code arbitraire à distance sur un serveur apache vulnérable.

Pour que la vulnérabilité puisse être exploitée, deux conditions doivent être réunies :

- l'option `FakeBasicAuth` est activée ;
- le certificat client est valide (autorité de certification reconnue par le serveur).

## 5 Solution

Appliquer les correctifs à partir des sources :

- pour Apache 1.3.x :  
[http://www.modssl.org/source/mod\\_ssl-2.8.18-1.3.31.tar.gz](http://www.modssl.org/source/mod_ssl-2.8.18-1.3.31.tar.gz)
- pour Apache 2.0.x :  
[http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl\\_engine\\_kernel.c?r1=1.105&r2=1.106](http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_kernel.c?r1=1.105&r2=1.106)

Pour OpenBSD, appliquer les correctifs :

- Pour OpenBSD 3.5, le correctif est téléchargeable à l'adresse suivante :  
[ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/013\\_httpd.patch](ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/013_httpd.patch)
- pour OpenBSD 3.4, le correctif est téléchargeable à l'adresse suivante :  
[ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/025\\_httpd3.patch](ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.4/common/025_httpd3.patch)

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Mandrake MDKSA-2004:054 du 01 juin 2004 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:054>
- Bulletin de sécurité Mandrake MDKSA-2004:055 du 01 juin 2004 :  
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:055>
- Bulletin de sécurité RedHat RHSA-2004:245 du 14 juin 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-245.html>
- Bulletin de sécurité RedHat RHSA-2004:342 du 06 juillet 2004 :  
<http://rhn.redhat.com/errata/RHSA-2004-342.html>
- Bulletin de sécurité Gentoo GLSA 200406-05 du 09 juin 2004 :  
<http://www.gentoo.org/security/en/glsa/glsa-200406-05.xml>
- Bulletin de sécurité OpenBSD du 12 juin 2004 :  
<http://www.openbsd.org/errata.html#httpd>  
<http://www.openbsd.org/errata34.html>
- Mise à jour de sécurité des paquetages NetBSD apache et apache2 :  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/apache/README.html>  
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/apache2/README.html>
- Bulletin de sécurité Apple du 07 septembre 2004 :  
<http://docs.info.apple.com/article.html?artnum=61798>
- Référence CVE CAN-2004-0488 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0488>

## Gestion détaillée du document

**02 juin 2004** version initiale.

**10 juin 2004** ajout de la référence au bulletin de sécurité Gentoo.

**14 juin 2004** ajout de la référence au bulletin de sécurité OpenBSD.

**15 juin 2004** ajout de la référence au bulletin de sécurité RedHat.

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

**06 juillet 2004** ajout d'une seconde référence au bulletin de sécurité RedHat.

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