



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 janvier 2005
N° CERTA-2004-AVI-247-006

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-247>

Gestion du document

Référence	CERTA-2004-AVI-247-006
Titre	Vulnérabilité du module Apache mod_ssl
Date de la première version	16 juillet 2004
Date de la dernière version	20 janvier 2004
Source(s)	Mise à jour de sécurité mod_ssl du 16 juillet 2004
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

Toutes les versions du module Apache mod_ssl antérieures à la version 2.8.19.

3 Résumé

Une vulnérabilité dans mod_ssl permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

4 Description

Une vulnérabilité de type débordement de mémoire est présente dans la fonction `ssl_log()` du module `mod_ssl` d'Apache.

Un utilisateur mal intentionné peut ainsi réaliser un déni de service ou exécuter du code arbitraire à distance sur un serveur Apache vulnérable.

5 Solution

- Appliquer le correctif à partir des sources pour mettre à jour mod_ssl en version 2.8.19 :
http://www.modssl.org/source/mod_ssl-2.8.19-1.3.31.tar.gz
- Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site Internet de mod_ssl :
<http://www.modssl.org>
- Site Internet des mises à jour de mod_ssl :
<http://www.modssl.org/news/>
- Site Internet du serveur web Apache :
<http://httpd.apache.org>
- Bulletin de sécurité Gentoo GLSA 200407-18 du 22 juillet 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200407-18.xml>
- Bulletin de sécurité Debian DSA-532 du 22 juillet 2004 :
<http://www.debian.org/security/2004/dsa-532>
- Bulletin de sécurité Mandrake MDKSA-2004:075 du 27 juillet 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:075>
- Mise à jour de sécurité du paquetage NetBSD ap-ssl :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/ap-ssl/README.html>
- Bulletin de sécurité FreeBSD "apache13-modssl –format string vulnerability in proxy support" du 17 octobre 2004 :
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité pour "VMware ESX Server 2.1.2" :
<http://www.vmware.com/download/esx/esx212-10921update.html>
- Mise à jour de sécurité pour "VMware ESX Server 2.0.1" :
<http://www.vmware.com/download/esx/esx201-11429update.html>
- Mise à jour de sécurité pour "VMware ESX Server 1.5.2" :
<http://www.vmware.com/download/esx/esx152-10816update.html>
- Référence CVE CAN-2004-0700 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0700>

Gestion détaillée du document

16 juillet 2004 version initiale.

19 juillet 2004 ajout de la référence à la mise à jour NetBSD pour ap-ssl.

22 juillet 2004 ajout de la référence au bulletin de sécurité Gentoo.

23 juillet 2004 ajout de la référence au bulletin de sécurité Debian. Ajout référence CVE.

28 juillet 2004 ajout de la référence au bulletin de sécurité Mandrake.

18 octobre 2004 ajout de la référence au bulletin de sécurité FreeBSD.

20 janvier 2005 ajout de la référence aux mises à jour de sécurité VMware.