

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Apache-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-2008-AVI-178>

Gestion du document

Référence	CERTA-2008-AVI-178
Titre	Vulnérabilité dans Apache-SSL
Date de la première version	03 avril 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apache-SSL AKLINK-SA-2008-005 du 02 avril 2008
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

- Atteinte à l'intégrité des données à distance ;
- atteinte à la confidentialité des données à distance.

2 Systèmes affectés

Apache-SSL versions antérieures à la version apache_1.3.41+ssl_1.59.

3 Résumé

Une vulnérabilité a été découverte dans Apache-SSL permettant d'interagir avec des données en mémoire.

4 Description

Apache-SSL est un serveur web construit à partir du serveur Apache, et d'OpenSSL.

Une vulnérabilité a été découverte dans ce serveur. Cette vulnérabilité est due à une mauvaise gestion de certaines données contenues dans les certificats clients. Elle peut être exploitée par un utilisateur malveillant afin de réécrire ou faire afficher des parties de la mémoire.

5 Solution

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

6 Documentation

- Bulletin de sécurité Apache-SSL AKLINK-SA-2008-005 du 02 avril 2008 :
<http://www.apache-ssl.org/advisory-cve-2008-0555.txt>
- Référence CVE CVE-2008-0555 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0555>

Gestion détaillée du document

03 avril 2008 version initiale.