

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité SSL sous Apache

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-2002-AVI-049>

Gestion du document

Référence	CERTA-2002-AVI-049
Titre	Vulnérabilité SSL sous Apache
Date de la première version	05 mars 2002
Date de la dernière version	–
Source(s)	Liste de diffusion Bugtraq
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.

2 Systèmes affectés

- Versions du module `mod_ssl` antérieures à la version 2.8.7-1.3.23;
- versions de `Apache-ssl` antérieures à la version 1.3.22-1.47.

3 Résumé

Une vulnérabilité de type « débordement de mémoire » présente dans le module `mod_ssl` et `apache-ssl` permet à un utilisateur mal intentionné l'exécution de code arbitraire à distance.

4 Description

SSL permet l'utilisation de connexions sécurisées sur des serveurs web (`https://`) ou autres serveurs sécurisés (`ftps://`).

Une vulnérabilité de type « débordement de mémoire » à été découverte dans le mécanisme de gestion de cache de sessions.

Cette vulnérabilité permet à un utilisateur mal intentionné de réaliser l'exécution de code arbitraire à distance.

5 Contournement provisoire

Désactiver le paramètre `-DSSL` dans le script `httpd` en attendant d'appliquer les correctifs.

6 Solution

Installer les correctifs disponibles sur

<http://www.apache-ssl.org/> et sur

<http://www.modssl.org/>

7 Documentation

- Message de Ed Moyle sur la liste de diffusion BugTraq
<http://online.securityfocus.com/archive/1/258646>
- Avis de sécurité Apache-SSL
<http://www.apache-ssl.org/advisory-20020301.txt>
- Avis de sécurité ESA-20020301-005 de EnGarde Secure Linux
<http://www.engardelinux.org>
- Avis de sécurité 2002-0034 de Trustix Secure Linux
<http://www.trustix.net/pub/Trustix/updates/>

Gestion détaillée du document

05 mars 2002 version initiale.