



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 mai 2004
N° CERTA-2004-AVI-029-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur HTTP 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-2004-AVI-029>

Gestion du document

Référence	CERTA-2004-AVI-029-001
Titre	Vulnérabilité du serveur HTTP Apache-SSL
Date de la première version	10 février 2004
Date de la dernière version	12 mai 2004
Source(s)	Avis de sécurité d'Apache-SSL du 06 février 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

Accès non autorisé au serveur HTTP Apache-SSL.

2 Systèmes affectés

Serveur HTTP Apache-SSL versions 1.3.28+1.52 et antérieures.

3 Résumé

Une vulnérabilité dans le serveur HTTP Apache-SSL permet à un utilisateur mal intentionné d'accéder au serveur sans autorisation.

4 Description

Apache-SSL est un serveur HTTP basé sur le serveur HTTP Apache et SSLeay/OpenSSL.

A l'aide de l'instruction *SSLVerifyClient*, il est possible de vérifier la présence d'un certificat côté client. Pour cela, le serveur nécessite un fichier contenant, pour chaque utilisateur autorisé à se connecter, le *Distinguished Name* (DN) du client, et le chiffrement du mot de passe par défaut *password* (la chaîne chiffrée est *xxj31ZMTZzkVA*).

Dans le cas où le certificat client est optionnel (la valeur de l'instruction *SSLVerifyClient* fixée à "1" ou à "3"), et si la directive *SSLFakeBasicAuth* est activée, il est alors possible pour une personne mal intentionnée d'usurper l'identité d'un utilisateur (le DN) pour se connecter au serveur.

5 Solution

La version 1.3.29+1.53 corrige cette vulnérabilité. Elle est disponible sur le site d'Apache-SSL (cf. section Documentation).

6 Documentation

Site du serveur HTTP Apache-SSL :
<http://www.apache-ssl.org>

Avis de sécurité d'Apache-SSL du 06 février 2004 :
<http://www.apache-ssl.org/advisory-20040206.txt>

Avis de sécurité FreeBSD du 10 février 2004 :
<http://www.vuxml.org/freebsd/>

Gestion détaillée du document

10 février 2004 version initiale.

12 mai 2004 ajout référence au bulletin de sécurité FreeBSD.