Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 octobre 2001
N° CERTA-2001-AVI-131

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du serveur Apache

Gestion du document

Référence	CERTA-2001-AVI-131
Titre	Vulnérabilités du serveur Apache
Date de la première version	26 octobre 2001
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risques

– Destruction d'informations ;
– accès à des informations confidentielles.

2 Systèmes affectés

Serveurs HTTP Apache version 1.3.20 et antérieures.

3 Résumé

Il existe deux vulnérabilités dans le serveur HTTP Apache, permettant à un utilisateur mal intentionné de récupérer des informations sur le système ou d'écraser des fichiers existants.

4 Description

La première vulnérabilité concerne le programme *split-logfile*. Ce programme écrit en Perl sert à traiter les fichiers de logs. Une vulnérabilité de ce programme permet à un utilisateur mal intentionné d'écraser n'importe

quel fichier ayant une extension *.log*.

La deuxième vulnérabilité concerne le module *mod_negotiation*. Un utilisateur mal intentionné peut, à l'aide d'une URL habilement choisie, contourner le mécanisme de ce module et obtenir des informations sur la structure des fichiers du serveur.

5 Contournement provisoire

Concernant le programme *split-logfile*, il faut le désactiver s'il n'est pas utilisé.
Pour se protéger de la vulnérabilité du module *mod_negotiation*, il faut désactiver les options *Indexes* et *Multiviews*.

6 Solution

Ces vulnérabilités ont été corrigées dans la version 1.3.21.

7 Documentation

Suivi des évolutions du serveur HTTP Apache :
http://httpd.apache.org/dist/httpd/CHANGES_1.3

Gestion détaillée du document

26 octobre 2001 version initiale.