

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2009-AVI-424>

Gestion du document

Référence	CERTA-2009-AVI-424
Titre	Multiples vulnérabilités dans Apache
Date de la première version	07 octobre 2009
Date de la dernière version	–
Source(s)	Liste des changements apportés à la version 2.2.14 de Apache
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

- Dénis de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les versions antérieures à Apache 2.2.14.

3 Résumé

Plusieurs vulnérabilités présentes dans Apache ont été corrigées. Ces vulnérabilités permettent de provoquer un déni de service à distance ou de contourner la politique de sécurité.

4 Description

Trois vulnérabilités ont été corrigées dans Apache :

- Deux vulnérabilités concernent le module `mod_proxy_ftp`. La première est de type pointeur nul et peut provoquer un déni de service par le biais d'un serveur FTP construit de manière particulière. La seconde

permet à un attaquant d'envoyer des commandes FTP arbitraires en utilisant le serveur Apache en tant que serveur mandataire ;

- une troisième vulnérabilité concernant un bogue dans l'APR (Apache Portable Runtime) permet à un attaquant de provoquer un déni de service distant sur les serveurs Sun Solaris.

5 Solution

La version Apache 2.2.14 corrige ces vulnérabilités :

<http://httpd.apache.org/download.cgi>

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

6 Documentation

- Liste des changements apportés à la version 2.2.14 de Apache :
http://httpd.apache.org/security/vulnerabilities_22.html
- Référence CVE CVE-2009-3094 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3094>
- Référence CVE CVE-2009-3095 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3095>
- Référence CVE CVE-2009-2699 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2699>

Gestion détaillée du document

07 octobre 2009 version initiale.