



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 février 2012
N° CERTA-2012-AVI-050

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2012-AVI-050>

Gestion du document

Référence	CERTA-2012-AVI-050
Titre	Vulnérabilités dans Apache
Date de la première version	02 février 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apache du 31 janvier 2012
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 ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

Apache HTTP Server versions inférieures à 2.2.22.

3 Résumé

Plusieurs vulnérabilités permettant de porter atteinte à la confidentialité des données, causer un déni de service et d'élever ses privilèges sont présentes dans *Apache HTTP Server*.

4 Description

Plusieurs vulnérabilités existent dans *Apache HTTP Server*. Elles permettent à un utilisateur malintentionné de porter atteinte à la confidentialité des données, causer un déni de service et d'élever ses privilèges. La liste

ci-dessous fournit le détail de ces vulnérabilités :

- CVE-2011-3368 : une erreur dans la gestion d'URI mal formées par le module *mod_proxy* permet à une personne malintentionnée d'envoyer des requêtes à des machines du réseau interne depuis l'extérieur ;
- CVE-2011-3607 : la fonction *ap_pregsub*, lorsque le module *mod_setenvif* est activé, est vulnérable à un dépassement d'entier permettant à un utilisateur malintentionné d'élever ses privilèges ;
- CVE-2011-4317 : cette vulnérabilité permet à un utilisateur malintentionné d'accéder à des machines du réseau interne depuis l'extérieur.
- CVE-2012-0021 : *mod_log_config* ne gère pas correctement certains *cookies*, ce qui peut conduire à un arrêt inopiné du service *Apache*.
- CVE-2012-0031 : un problème dans la gestion des segments de mémoire partagée peut conduire à un déni de service local.
- CVE-2012-0053 : lorsqu'aucune page personnalisée n'est définie pour le code d'erreur 400, il est possible d'obtenir les *cookies httpOnly*.

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 du 31 janvier 2012 :
http://mail-archives.apache.org/mod_mbox/httpd-announce/201201.mbox/<4F286C70.9040705@apache.org>
- Référence CVE CVE-2011-3368 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3368>
- Référence CVE CVE-2011-3607 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3607>
- Référence CVE CVE-2011-4317 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-4317>
- Référence CVE CVE-2012-0021 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0021>
- Référence CVE CVE-2012-0031 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0031>
- Référence CVE CVE-2012-0053 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0053>

Gestion détaillée du document

02 février 2012 version initiale.