

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités du serveur HTTP 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-2003-AVI-095>

Gestion du document

Référence	CERTA-2003-AVI-095
Titre	Multiples vulnérabilités du serveur HTTP Apache
Date de la première version	02 juin 2003
Date de la dernière version	–
Source(s)	Annonce Apache 2.0.46 Bulletin de sécurité d'iDEFENSE "Apache portable runtime denial of service and arbitrary code execution vulnerability"
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

- Déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Apache versions 2.0.40 à 2.0.45 pour la vulnérabilité du module HTTP Basic Authentication ;
- Apache versions 2.0.37 à 2.0.45 pour la vulnérabilité dans la bibliothèque APR (Apache Portable Runtime).

3 Résumé

Deux vulnérabilités présentes dans le serveur HTTP Apache peuvent être exploitées par un utilisateur mal intentionné afin de réaliser un déni de service.

4 Description

4.1 vulnérabilité du module HTTP Basic Authentication

Une vulnérabilité présente dans le module HTTP Basic Authentication peut être exploitée par un utilisateur mal intentionné afin de réaliser un déni de service en interdisant l'accès à tout document protégé par un mot de passe.

4.2 Vulnérabilité dans la bibliothèque APR (Apache Portable Runtime)

APR (Apache Portable Runtime) est une bibliothèque utilisée par plusieurs modules notamment `mod_dav`. Une vulnérabilité de type fuite de mémoire présente dans la routine `apr_pspprintf` peut être exploitée par un utilisateur mal intentionné afin de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

5 Solution

Installer la version 2.0.46 d'Apache :

<http://httpd.apache.org>

ou appliquer le correctif de l'éditeur :

- Bulletin de sécurité MDKSA-2003:063 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:063>
- Bulletin de sécurité RHSA-2003:186 de Red Hat :
<http://rhn.redhat.com/errata/RHSA-2003-186.html>

6 Documentation

- Annonce de la version 2.0.46 d'Apache :
<http://www.apache.org/dist/httpd/Announcement2.html>
- Bulletin de sécurité d'iDEFENSE "Apache portable runtime denial of service and arbitrary code execution vulnerability" :
<http://www.idefense.com/advisory/05.30.03.txt>
- Référence CVE CAN-2003-0189 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0189>
- Référence CVE CAN-2003-0245 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0245>

Gestion détaillée du document

02 juin 2003 version initiale.