

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur 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-2002-AVI-130>

Gestion du document

| | |
|-----------------------------|----------------------------|
| Référence | CERTA-2002-AVI-130-003 |
| Titre | Vulnérabilité sur Apache |
| Date de la première version | 18 juin 2002 |
| Date de la dernière version | 11 juillet 2002 |
| Source(s) | Avis CA-2002-17 du Cert-CC |
| 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 ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Apache versions 1.3.x jusqu'à la version 1.3.24 incluse ;
- Apache versions 2.0.x jusqu'à la version 2.0.36 incluse.

3 Résumé

Une vulnérabilité dans le traitement de certaines requêtes sur Apache permet à un utilisateur mal intentionné d'effectuer un déni de service ou d'exécuter du code arbitraire.

4 Description

Avec le protocole HTTP 1.1, il est possible d'utiliser l'algorithme *chunk* lorsque la taille des données à envoyer au serveur n'est pas connue à l'avance.

Une vulnérabilité présente dans la routine de traitement des requêtes utilisant cet algorithme peut provoquer l'arrêt du processus fils traitant cette requête.

Dans les versions 2.0.x du serveur Apache, cette vulnérabilité ne peut pas être exploitée pour exécuter du code sur le serveur, mais peut provoquer un déni de service par l'arrêt et le redémarrage de nombreux processus.

Les plates-formes Windows et Netware sont plus sensibles que les autres à ce phénomène.

Dans les versions 1.3.x du serveur, il est en revanche possible de provoquer, par cette vulnérabilité, un débordement de pile et d'exécuter du code arbitraire.

5 Solution

Les versions 1.3.26 et 2.0.39 corrigent la vulnérabilité.

Consulter votre éditeur pour obtenir une mise à jour ou télécharger un correctif sur le site Apache Software Foundation (cf. Documentation).

6 Documentation

Avis CA-2002-17 du Cert-CC :

<http://www.cert.org/advisories/CA-2002-17.html>

Site Apache Software Foundation :

<http://httpd.apache.org>

Avis SGI 20020605-01-A :

<ftp://patches.sgi.com/support/free/security/advisories/20020605-01-A>

Avis Debian DSA-131-2 :

<http://www.debian.org/security/2002/dsa-131>

Avis SuSE SuSE-SA:2002:022 :

<http://www.suse.de/de/support/security/>

Avis RedHat RHSA-2002-103 :

<http://www.redhat.com/apps/support/errata/>

Avis Hewlett Packard HPSBUX0207-197 :

<http://www.itresourcecenter.hp.com/>

Gestion détaillée du document

18 juin 2002 version initiale.

19 juin 2002 première révision : ajout de précisions sur la vulnérabilité et de l'avis SGI.

20 juin 2002 deuxième révision : ajout des avis RedHat, SuSE et Debian.

11 juillet 2002 troisième révision : ajout de l'avis Hewlett Packard.