Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 février 2004
N° CERTA-2003-AVI-177-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du serveur HTTP Apache

Gestion du document

Référence	CERTA-2003-AVI-177-005
Titre	Vulnérabilités du serveur HTTP Apache
Date de la première version	30 octobre 2003
Date de la dernière version	23 février 2004
Source(s)	Avis de sécurité 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

- Divulgation d'informations ;
- élévation de privilèges ;
- exécution de code arbitraire.

2 Systèmes affectés

- Serveur HTTP Apache 2.0.x versions 2.0.47 et antérieures ;
- Serveur HTTP Apache 1.3.x versions 1.3.28 et antérieures.

3 Résumé

Deux vulnérabilités ont été découvertes dans certains modules du serveur HTTP Apache.

4 Description

Des vulnérabilités ont été découvertes sur le module *mod_cgid* d'une part, et sur les modules *mod_alias* et *mod_rewrite* d'autre part.

Le module *mod_cgid* ne traite pas correctement les sockets de type AF_UNIX qui sont utilisées pour la communication entre le démon *cgid* et le script CGI. La sortie du script CGI risque alors d'être envoyée au mauvais client.
Cette vulnérabilité n'affecte que les versions 2.0.x du serveur HTTP Apache.

Les modules *mod_alias* et *mod_rewrite* présentent des vulnérabilités de type débordement de mémoire dans certains cas de configuration d'expressions régulières.

5 Solution

Mettre à jour le serveur HTTP Apache en version 2.0.48 ou 1.3.29.

6 Documentation

Site du serveur HTTP Apache :
http://httpd.apache.org

Référence CVE CAN-2003-0789 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0789

Référence CVE CAN-2003-0542 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0542

Avis de sécurité Gentoo :
http://www.securityfocus.com/archive/1/345060/2003-11-18/2003-11-24/0

Avis de sécurité de Mandrake :
http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:103

Avis de sécurité de RedHat :
http://rhn.redhat.com/errata/RHSA-2003-320.html

Avis de sécurité HPSBUX0311-301 et HPSBUX0401-305 de HP pour HP-UX :
http://itrc.hp.com

Mise-à-jour 2004-01-26 pour Mac OS X 10.2.8 et Mac OS X 10.3.2 d'Apple :
http://docs.info.apple.com/article.html?artnum=61798

Bulletin de sécurité #57496 de Sun :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57496

Gestion détaillée du document

30 octobre 2003 version initiale.
21 novembre 2003 ajout de la référence à l'avis de sécurité Gentoo.
17 décembre 2003 ajout des références aux avis de sécurité de Mandrake, RedHat et HP.
29 janvier 2004 ajout de la référence à la mise-à-jour 2004-01-26 d'Apple.
12 février 2004 ajout de la référence au bulletin de sécurité de Sun.
23 février 2004 ajout de la référence à un avis HP (HPSBUX0401-305).