Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 octobre 2004
N° CERTA-2004-AVI-313-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités du serveur http Apache 2.0.x

Gestion du document

Référence	CERTA-2004-AVI-313-002
Titre	Vulnérabilités du serveur http Apache 2.0.x
Date de la première version	15 septembre 2004
Date de la dernière version	08 octobre 2004
Source(s)	Bulletin de sécurité SUSE
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.

2 Systèmes affectés

Apache versions 2.0.x antérieures à la version 2.0.51.

3 Résumé

Cinq vulnérabilités ont été découvertes dans le serveur http Apache.

4 Description

– Deux vulnérabilités sont présentes dans le module `mod_ssl` d'Apache. Une première vulnérabilité dans la fonction `char_buffer_read` peut être exploitée par un utilisateur mal intentionné pour exécuter un déni de service sur le serveur http (CVE CAN-2004-0751). Une deuxième vulnérabilité peut provoquer un déni de service par consommation excessive des ressources processeur (CVE CAN-2004-0748).

– Une vulnérabilité est présente dans le module `mod_dav` (module utilisé pour les accès webdav au le serveur web Apache). Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné pour réaliser un déni de service si le serveur web est configuré pour la gestion de processus léger (`thread`) et si cet utilisateur peut utiliser la méthode LOCK sur le système vulnérable (CVE CAN-2004-0809).
– Une vulnérabilité a été découverte dans la gestion des adresses IPv6 (CVE CAN-2004-0786).
– Une vulnérabilité de type débordement de mémoire permet à un utilisateur mal intentionné, par le biais d'un fichier *.htaccess* malicieusement construit, d'obtenir les droits d'un processus fils *httpd* (CVE CAN-2004-0747).

5 Solution

La version 2.0.51 du serveur http Apache corrige ces vulnérabilités.

6 Documentation

– Site internet du serveur http Apache :
http://www.apache.org
– Bulletin de sécurité Gentoo GLSA-200409-21 du 16 septembre 2004 :
http://www.gentoo.org/security/en/glsa/glsa-200409-21.xml
– Bulletin de sécurité Mandrake MDKSA-2004:096 du 15 septembre 2004 :
http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:096
– Bulletin de sécurité RedHat RHSA-2004:402 du 15 septembre 2004 :
http://rhn.redhat.com/errata/RHSA-2004-463.html
– Bulletin de sécurité SUSE SUSE-SA:2004:030 du 6 septembre 2004 :
http://www.suse.com/de/security/2004_30_apache2.html
– Bulletin de sécurité Debian DSA-558 du 6 octobre 2004 :
http://www.debian.org/security/2004/dsa-558
– Bulletin de sécurité FreeBSD pour apache du 15 septembre 2004 :
http://www.vuxml.org/freebsd/
– Mise à jour de sécurité du paquetage NetBSD apache2 du 14 septembre 2004 :
ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/apache2/README.html
– Référence CVE CAN-2004-0751 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0751
– Référence CVE CAN-2004-0809 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0809
– Référence CVE CAN-2004-0786 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0786
– Référence CVE CAN-2004-0747 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0747
– Référence CVE CAN-2004-0748 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0748

Gestion détaillée du document

15 septembre 2004 version initiale.

17 septembre 2004 Prise en compte de la sortie de la version 2.0.51 d'Apache : ajout des vulnérabilités CVE CAN-2004-0786, CAN-2004-0747 et CAN-2004-0748. Ajout des références aux bulletins de sécurité Gentoo, Mandrake, RedHat et FreeBSD.

08 octobre 2004 Ajout de la référence au bulletin de sécurité Debian.