



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 février 2005
N° CERTA-2004-AVI-370-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2004-AVI-370>

Gestion du document

Référence	CERTA-2004-AVI-370-003
Titre	Vulnérabilités du serveur HTTP Apache
Date de la première version	19 novembre 2004
Date de la dernière version	14 février 2005
Source(s)	Bulletin de sécurité Debian DSA-594 du 17 novembre 2004
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

- Exécution de code arbitraire ;
- déni de service.

2 Systèmes affectés

- Vulnérabilité CAN-2004-0940 : serveur HTTP Apache versions 1.3.32 et antérieures.
- Vulnérabilité CAN-2004-0942 : serveur HTTP Apache versions 2.0.52 et antérieures.

3 Résumé

Deux vulnérabilités ont été découvertes dans le serveur HTTP Apache.

4 Description

- Vulnérabilité CAN-2004-0940 : une vulnérabilité du module *mod_include* de type débordement de mémoire permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

Pour exploiter cette vulnérabilité, l'utilisateur doit être autorisé à créer des fichiers de type *Server Side Include (SSI)*.

- Vulnérabilité CAN-2004-0942 : une vulnérabilité a été découverte dans la gestion de certaines requêtes HTTP. Cette vulnérabilité peut être exploitée par un utilisateur distant mal intentionné afin de provoquer un déni de service.

5 Solution

La version 1.3.33 corrige la vulnérabilité CAN-2004-0940.
La version 2.0.53-dev corrige la vulnérabilité CAN-2004-0942.

6 Documentation

- Site Internet du serveur HTTP Apache :
<http://httpd.apache.org>
- Bulletin de sécurité d'Apache du 16 novembre 2004 (CAN-2004-0940) :
<http://www.apacheweek.com/features/security-13>
- Bulletin de sécurité d'Apache du 22 octobre 2004 (CAN-2004-0942) :
<http://www.apacheweek.com/features/security-20>
- Bulletin de sécurité Gentoo GLSA-200411-18 du 10 novembre 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200411-18.xml>
- Bulletin de sécurité Debian DSA-594 du 17 novembre 2004 :
<http://www.debian.org/security/2004/dsa-594>
- Bulletin de sécurité Mandrake MDKSA-2004:134 du 15 novembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:134>
- Bulletin de sécurité Mandrake MDKSA-2004:135 du 15 novembre 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:135>
- Bulletin de sécurité RedHat RHSA-2004:562 du 12 novembre 2004 :
<http://rhn.redhat.com/errata/RHSA-2004-562.html>
- Bulletin de sécurité SUSE SUSE-SR:2004:001 du 24 novembre 2004 :
http://www.suse.de/de/security/2004_01_sr.html
- Bulletin de sécurité HP HPSBTU01106 "HP Tru64 UNIX SWS (Apache) Secure Web Server remote denial of service (DoS)" du 22 décembre 2004 :
<http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01106>
- Mise à jour de sécurité des paquetages NetBSD apache et apache2 :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/apache/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/www/apache2/README.html>
- Référence CVE CAN-2004-0940 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0940>
- Référence CVE CAN-2004-0942 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0942>

Gestion détaillée du document

19 novembre 2004 version initiale.

25 novembre 2004 ajout de la référence au bulletin de sécurité SUSE.

03 janvier 2005 ajout de la référence au bulletin de sécurité HPSBTU01106 pour Apache sur Tru64 UNIX.

14 février 2005 ajout de la référence au bulletin de sécurité NetBSD.