

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de 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-2005-AVI-280>

Gestion du document

Référence	CERTA-2005-AVI-280-004
Titre	Vulnérabilités de Apache
Date de la première version	26 juillet 2005
Date de la dernière version	26 septembre 2005
Source(s)	Bulletin de sécurité RedHat RHSA-2005:582 du 25 juillet 2005
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 ;
- contournement de la politique de sécurité ;
- corruption de cache ;
- cross-site scripting.

2 Systèmes affectés

Apache version 2.0.54 et versions antérieures.

3 Description

- Une première vulnérabilité de type débordement de mémoire dans une fonction de gestion des listes de révocation de certificats (CRL) permet à un attaquant de créer un déni de service sur le serveur Apache vulnérable (CVE CAN-2005-1268) ;
- une seconde vulnérabilité, lorsque Apache est utilisé comme un proxy, permet à un attaquant de contourner la politique de sécurité, corrompre le cache ou réaliser des attaques de type cross-site scripting (CVE CAN-2005-2088).

4 Solution

La future version Apache 2.0.55 corrigera ces vulnérabilités.
Apache peut être téléchargé à l'adresse suivante :

<http://httpd.apache.org/download.cgi> Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Site Internet du serveur HTTP Apache :
<http://httpd.apache.org>
- ASF Bugzilla Bug #35081 :
http://issues.apache.org/bugzilla/show_bug.cgi?id=35081
- Document sur le HTTP Request Smuggling :
<http://www.watchfire.com/resources/HTTP-Request-Smuggling.pdf>
- Bulletin de sécurité RedHat RHSA-2005:582 du 25 juillet 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-582.html>
- Bulletin de sécurité FreeBSD pour apache, apache+ipv6, apache_fp, apache+ssl, apache+mod_perl, apache+mod_ssl, apache+mod_ssl+ipv6 du 26 juillet 2005 :
<http://www.vuxml.org/freebsd/pkg-apache.html>
<http://www.vuxml.org/freebsd/pkg-apache+ipv6.html>
http://www.vuxml.org/freebsd/pkg-apache_fp.html
<http://www.vuxml.org/freebsd/pkg-apache+ssl.html>
http://www.vuxml.org/freebsd/pkg-apache+mod_perl.html
http://www.vuxml.org/freebsd/pkg-apache+mod_ssl.html
http://www.vuxml.org/freebsd/pkg-apache+mod_ssl+ipv6.html
- Bulletin de sécurité SUSE SUSE-SR:2005:018 du 28 juillet 2005 :
http://www.novell.com/linux/security/advisories/2005_18_sr.html
- Bulletin de sécurité Debian DSA-803 :
<http://www.debian.org/security/2005/dsa-803>
- Mise à jour de sécurité Fedora Core 3 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Mise à jour de sécurité Fedora Core 4 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/>
- Mise à jour pour IBM « Hardware Management Console » (HMC) :
 - Version 3.3.2 et supérieures :
http://www-1.ibm.com/support/docview.wss?uid=isg1SSRVHMCHMC_S081514_52
 - Version V4R2.0 et supérieures :
http://www-1.ibm.com/support/docview.wss?uid=isg1SSRVHMCHMC_S081514_252
- Référence CVE CAN-2005-1268 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1268>
- Référence CVE CAN-2005-2088 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2088>

Gestion détaillée du document

26 juillet 2005 version initiale.

28 juillet 2005 ajout des références aux bulletins de sécurité FreeBSD.

29 juillet 2005 ajout de la référence au bulletin de sécurité SUSE SUSE-SR:2005:018.

09 septembre 2005 ajout de la référence au bulletin de sécurité Debian DSA-803 et Fedora.

26 septembre 2005 ajout des bulletins IBM HMC.