



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 novembre 2007
N° CERTA-2007-AVI-402-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples 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-2007-AVI-402>

Gestion du document

Référence	CERTA-2007-AVI-402-001
Titre	Multiples vulnérabilités de Apache
Date de la première version	13 septembre 2007
Date de la dernière version	08 novembre 2007
Source(s)	Bulletin de version 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

- Déni de service à distance ;
- injection de code indirecte ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Serveur *Apache* versions 2.2.x et 2.0.x.

3 Résumé

Plusieurs vulnérabilités du serveur web *Apache* permettent à un utilisateur malintentionné de provoquer un déni de service à distance, de réaliser de l'injection de code indirecte et d'accéder à des informations sensibles.

4 Description

Plusieurs vulnérabilités affectent le serveur web *Apache* :

- une erreur dans la fonction `recall_headers` du module `mod_mem_cache` permet à un utilisateur malintentionné d'accéder à des informations qui peuvent être sensibles ;

- une erreur dans le module `mod_cache` se traduit par l'arrêt inopiné (*crash*) d'un processus fils lors du traitement de certaines requêtes. Cette erreur permet à un utilisateur malintentionné de provoquer un déni de service à distance ;
- le serveur HTTP ne vérifie pas qu'un processus est un processus fils Apache avant de lui envoyer un signal. Cette absence de vérification permet à un utilisateur local malintentionné, dans certaines conditions, de provoquer un déni de service ;
- une erreur dans le module `mod_proxy` est exploitable par un utilisateur malintentionné pour provoquer, dans certaines circonstances, un déni de service à distance ;
- une erreur dans le module `mod_status` permet à un utilisateur malintentionné de réaliser de l'injection de code indirecte (*cross site scripting*) si la page d'état du serveur est publique et si le paramètre `ExtendedStatus` est activé.

5 Solution

Les versions 2.2.6 et 2.0.61 corrigent ces problèmes.

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletins de version Apache du 07 septembre 2007 :
http://httpd.apache.org/security/vulnerabilities_20.html
http://httpd.apache.org/security/vulnerabilities_22.html
- Bulletin de sécurité Gentoo GLSA-200711-06 du 07 novembre 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200711-06.xml>
- Bulletin de sécurité Ubuntu USN-499-1 du 16 août 2007 :
<http://www.ubuntu.com/usn/usn-499-1>
- Bulletin de sécurité Ubuntu USN-499-1 du 16 août 2007 :
<http://www.ubuntu.com/usn/usn-499-1>
- Bulletin de sécurité Mandriva MDKSA-2007:140 du 04 juillet 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:140>
- Bulletin de sécurité Red Hat RHSA-2007:0533 du 26 juin 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0533.html>
- Bulletin de sécurité Red Hat RHSA-2007:0534 du 26 juin 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0534.html>
- Bulletin de sécurité Red Hat RHSA-2007:0556 du 26 juin 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0556.html>
- Bulletin de sécurité Red Hat RHSA-2007:0662 du 13 juillet 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0662.html>
- Bulletins de sécurité IBM du 04 septembre 2007 :
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK50469>
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK50467>
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK49355>
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK49295>
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK52702>
<http://www-1.ibm.com/support/docview.wss?uid=swg1PK53984>
- Bulletin de sécurité HP-UX HPSBUX02262 SSRT071447 du 08 octobre 2007 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01178795>
- Bulletin de sécurité HP-UX HPSBUX02273 SSRT071476 du 12 octobre 2007 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01182588>
- Bulletin de sécurité Avaya du 17 août 2007 :
<http://support.avaya.com/elmodocs2/security/ASA-2007-351.htm>
<http://support.avaya.com/elmodocs2/security/ASA-2007-353.htm>
<http://support.avaya.com/elmodocs2/security/ASA-2007-363.htm>

- Référence CVE CVE-2007-1862 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1862>
- Référence CVE CVE-2007-1863 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1863>
- Référence CVE CVE-2007-3304 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3304>
- Référence CVE CVE-2007-3847 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3847>
- Référence CVE CVE-2007-5752 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5752>

Gestion détaillée du document

13 septembre 2007 version initiale.

08 novembre 2007 ajout de la référence au bulletin de sécurité Gentoo.