



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-339-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-339>

Gestion du document

Référence	CERTA-2007-AVI-339-002
Titre	Multiples vulnérabilités dans Apache
Date de la première version	01 août 2007
Date de la dernière version	08 novembre 2007
Source(s)	Bulletin de sécurité Apache du 31 juillet 2007
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 1.3.37 et antérieures ;
- Apache versions 2.0.59 et antérieures ;
- Apache versions 2.2.4 et antérieures.

3 Résumé

Plusieurs vulnérabilités sont présentes dans Apache et permettent à un utilisateur local de provoquer un déni de service et à un utilisateur distant de conduire une attaque de type « *Cross-Site Scripting* ».

4 Description

Trois vulnérabilités ont été identifiées dans le serveur web Apache :

- Une première faille dans les modules `mod_status` et `mod_autoindex` permet à un utilisateur distant de conduire une attaque de type « *Cross-Site Scripting* » ;

- une seconde dans le composant MPM (Multi-Processing Module) des versions 2.x de Apache permet à un utilisateur local au serveur de provoquer un arrêt inopiné de Apache ;
- une dernière vulnérabilité dans le module mod_cache permet à un utilisateur malintentionné distant de provoquer un arrêt de certains processus fils de Apache. Si le composant MPM (Multi-Processing Module) est utilisé, il est possible de provoquer un arrêt complet de Apache.

5 Solution

Se référer aux bulletins de sécurité des éditeurs pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletins de sécurité Apache du 31 juillet 2007 :
http://httpd.apache.org/security/vulnerabilities_22.html
http://httpd.apache.org/security/vulnerabilities_20.html
http://httpd.apache.org/security/vulnerabilities_13.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 Mandriva MDKSA-2007:140 du 04 juillet 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:140>
- Bulletin de sécurité Mandriva MDKSA-2007:141 du 04 juillet 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:141>
- Bulletin de sécurité Mandriva MDKSA-2007:142 du 04 juillet 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:142>
- Bulletin de sécurité RedHat RHSA-2007:0533 du 26 juillet 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0533.html>
- Bulletin de sécurité RedHat RHSA-2007:0534 du 26 juillet 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0534.html>
- Bulletin de sécurité RedHat RHSA-2007:0556 du 26 juillet 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0556.html>
- Bulletin de sécurité RedHat RHSA-2007:0662 du 26 juillet 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0662.html>
- Bulletin de sécurité Ubuntu USN-499-1 du 16 août 2007 :
<http://www.ubuntu.com/usn/usn-499-1>
- Référence CVE CVE-2006-5752 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5752>
- 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-2007-4465 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4465>

Gestion détaillée du document

01 août 2007 version initiale.

22 août 2007 ajout de la référence au bulletin de sécurité Ubuntu.

07 novembre 2007 ajout de la référence CVE-2007-4465 et de la référence au bulletin de sécurité Gentoo.