



CVE-2007-1863

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-1863
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-06-27 17:30:00 UTC
Updated	2023-02-13 02:17:00 UTC
Description	cache_util.c in the mod_cache module in Apache HTTP Server (httpd), when caching is enabled and a threaded Multi-Proc

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X Server	10.0	All	All	All
Operating System	Apple	Mac Os X Server	10.1	All	All	All
Operating System	Apple	Mac Os X Server	10.1.1	All	All	All
Operating System	Apple	Mac Os X Server	10.1.2	All	All	All
Operating System	Apple	Mac Os X Server	10.1.3	All	All	All
Operating System	Apple	Mac Os X Server	10.1.4	All	All	All
Operating System	Apple	Mac Os X Server	10.1.5	All	All	All
Operating System	Apple	Mac Os X Server	10.2	All	All	All
Operating System	Apple	Mac Os X Server	10.2.1	All	All	All
Operating System	Apple	Mac Os X Server	10.2.2	All	All	All
Operating System	Apple	Mac Os X Server	10.2.3	All	All	All
Operating System	Apple	Mac Os X Server	10.2.4	All	All	All
Operating System	Apple	Mac Os X Server	10.2.5	All	All	All
Operating System	Apple	Mac Os X Server	10.2.6	All	All	All
Operating System	Apple	Mac Os X Server	10.2.7	All	All	All
Operating System	Apple	Mac Os X Server	10.2.8	All	All	All
Operating System	Apple	Mac Os X Server	10.3	All	All	All

[illegible]

Operating System	Apple	Mac Os X Server	10.3	All	All	All
Operating System	Apple	Mac Os X Server	10.3.1	All	All	All
Operating System	Apple	Mac Os X Server	10.3.2	All	All	All
Operating System	Apple	Mac Os X Server	10.3.3	All	All	All
Operating System	Apple	Mac Os X Server	10.3.4	All	All	All
Operating System	Apple	Mac Os X Server	10.3.5	All	All	All
Operating System	Apple	Mac Os X Server	10.3.6	All	All	All
Operating System	Apple	Mac Os X Server	10.3.7	All	All	All
Operating System	Apple	Mac Os X Server	10.3.8	All	All	All
Operating System	Apple	Mac Os X Server	10.3.9	All	All	All
Operating System	Apple	Mac Os X Server	10.4	All	All	All
Operating System	Apple	Mac Os X Server	10.4.1	All	All	All
Operating System	Apple	Mac Os X Server	10.4.2	All	All	All
Operating System	Apple	Mac Os X Server	10.4.3	All	All	All
Operating System	Apple	Mac Os X Server	10.4.4	All	All	All
Operating System	Apple	Mac Os X Server	10.4.5	All	All	All
Operating System	Apple	Mac Os X Server	10.4.6	All	All	All
Operating System	Apple	Mac Os X Server	10.4.7	All	All	All
Operating System	Apple	Mac Os X Server	10.4.8	All	All	All
Operating System	Apple	Mac Os X Server	10.4.9	All	All	All

References
Reference
Red Hat update for httpd - Advisories - Secunia
Pony Mail!
Mandriva update for apache - Advisories - Secunia
issues.rpath.com/browse/RPL-1500
rh.n.redhat.com Red Hat Support
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Pony Mail!
2007-0026
rPath update for httpd and mod_ssl - Advisories - Secunia
Pony Mail!
rh.n.redhat.com Red Hat Support
Fedora update for httpd - Advisories - Secunia
Pony Mail!

37079
Pony Mail!
Apache HTTPD mod_cache May Let Remote Users Deny Service - SecurityTracker
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Security Announcement
Pony Mail!
Pony Mail!
[Security-announce] VMSA-2009-0010 VMware Hosted products update libpng and Apache HTTP Server
Pony Mail!
Pony Mail!
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Pony Mail!
Pony Mail!
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Pony Mail!
IBM WebSphere Application Server for z/OS HTTP Server Vulnerabilities - Advisories - Secunia
Apache Denial of Service and Cross-Site Scripting - Advisories - Secunia
244658 – (CVE-2007-1863) CVE-2007-1863 httpd mod_cache segfault
Pony Mail!
[Apache-SVN] Revision 535617
rhn.redhat.com Red Hat Support
ASA-2007-353 (RHSA-2007-0557)
US-CERT Technical Cyber Security Alert TA08-150A -- Apple Updates for Multiple Vulnerabilities
httpd 2.2 vulnerabilities - The Apache HTTP Server Project
Pony Mail!
SecurityFocus
Repository / Oval Repository
Avaya Products Perl Net::DNS and Apache Vulnerabilities - Advisories - Secunia
Gentoo Bug 186219 - www-servers/apache Multiple issues (CVE-2006-{5752}, CVE-2007-{1862,1863,3304,3847,4465})
PK52702: Z/OS IBM HTTP SERVER FOR WEBSPPHERE (POWERED BY APACHE) FIX PACK 6.1.0.13
Pony Mail!
Pony Mail!

Advisories Mandriva
Advisories Mandriva
Trustix Update for Multiple Packages - Advisories - Secunia
HP-UX update for Apache - Advisories - Secunia
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Pony Mail!
Interstage HTTP Server Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Webmail - OVH
SUSE update for apache2 - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Pony Mail!
Pony Mail!
HPSBUX02262 SSRT071447 rev. 1 - HP-UX running Apache, Remote Arbitrary Code Execution, Cross Site Scripting (XSS) - c01178795 - H
Pony Mail!
Pony Mail!
Pony Mail!
Apache HTTP Server Mod_Cache Denial of Service Vulnerability
Pony Mail!
Gentoo Linux Documentation -- Apache: Multiple vulnerabilities
APPLE-SA-2008-05-28 Security Update 2008-003 and Mac OS X v10.5.3
Ubuntu update for apache - Advisories - Secunia
rhn.redhat.com Red Hat Support
IBM PK49355: CVE-2007-1863 MOD_CACHE CRASH WITH MALICIOUS REQUEST
Apache httpd 2.0 vulnerabilities - The Apache HTTP Server Project
Pony Mail!
This page provides Security Information. : FUJITSU
Pony Mail!
Gentoo update for apache - Advisories - Secunia
Pony Mail!
Pony Mail!
USN-499-1: Apache vulnerabilities Ubuntu
Pony Mail!
[SECURITY] Fedora 7 Update: httpd-2.2.6-1.fc7
Pony Mail!
CVE Program record
NVD vulnerability detail



Vendor Comments And Credit

Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP Server 2.2.6 and 2.0.61: http://httpd.apache.org/security/vulnerabilities_2



There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report