



CVE-2007-6422

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

Summary

CVE	CVE-2007-6422
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-08 18:46:00 UTC
Updated	2023-11-07 02:01:00 UTC
Description	The balancer_handler function in mod_proxy_balancer in the Apache HTTP Server 2.2.0 through 2.2.6, when a threaded M

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	-	All	All	All
Application	Apache	Http Server	2.2	All	All	All
Application	Apache	Http Server	2.2.1	All	All	All
Application	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.3	All	All	All
Application	Apache	Http Server	2.2.4	All	All	All
Application	Apache	Http Server	2.2.6	All	All	All
Application	Apache	Http Server	-	All	All	All
Application	Apache	Http Server	2.2	All	All	All
Application	Apache	Http Server	2.2.1	All	All	All
Application	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.3	All	All	All
Application	Apache	Http Server	2.2.4	All	All	All
Application	Apache	Http Server	2.2.6	All	All	All

References

Reference	Source	Link
-----------	--------	------

Support / Security / Advisories / / MDVSA-2008:016 Mandriva	MANDRIVA	www.mandriva.com
SUSE update for apache and apache2 - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
[SECURITY] Fedora 7 Update: httpd-2.2.8-1.fc7	FEDORA	www.redhat.com
Apache 'mod_proxy_balancer' Multiple Vulnerabilities	BID	www.securityfocus.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Apache: Multiple vulnerabilities — Gentoo Linux Documentation	GENTOO	security.gentoo.org
Pony Mail!		lists.apache.org
Mandriva update for apache - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Fedora update for httpd - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
Pony Mail!		lists.apache.org
USN-575-1: Apache vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Gentoo update for apache - Advisories - Secunia	SECUNIA	secunia.com
rhn.redhat.com Red Hat Support	REDHAT	www.redhat.com
Webmail - OVH	VUPEN	www.vupen.com
httpd 2.2 vulnerabilities - The Apache HTTP Server Project	CONFIRM	httpd.apache.org
SecurityFocus	BUGTRAQ	www.securityfocus.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
SecurityFocus	CONFIRM	www.securityfocus.com

SecurityReason - Apache2 CSRF, XSS, Memory Corruption and Denial of Service vulnerability	SHEASON	securityreason.com
[SECURITY] Fedora 8 Update: httpd-2.2.8-1.fc8	FEDORA	www.redhat.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
[security-announce] SUSE Security Announcement: Apache,Apache2 security	SUSE	lists.opensuse.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Ubuntu update for apache2 - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP Server 2.2.8. http://httpd.apache.org/security/vulnerabilities_22.html
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