



CVE-2007-6420

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

Summary

CVE	CVE-2007-6420
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-12 00:46:00 UTC
Updated	2023-11-07 02:01:00 UTC
Description	Cross-site request forgery (CSRF) vulnerability in the balancer-manager in mod_proxy_balancer for Apache HTTP Server 2

Risk And Classification

Problem Types: CWE-352

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	2.2.0	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	2.2.0	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
Apache 'mod_proxy_balancer' Multiple Vulnerabilities	BID
Pony Mail!	

Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	
SecurityFocus	BUGTRAQ
Pony Mail!	
Pony Mail!	
Pony Mail!	
Pony Mail!	
Support	REDHAT
Pony Mail!	
Pony Mail!	MLIST
Pony Mail!	MLIST
Pony Mail!	MLIST
HP-UX update for Apache - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Pony Mail!	MLIST
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Pony Mail!	
RETIRED: Apple Mac OS X 2008-007 Multiple Security Vulnerabilities	BID
Pony Mail!	
About Security Update 2008-007	CONFIRM
Apache: Denial of Service — Gentoo Linux Documentation	GENTOO
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Pony Mail!	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
APPLE-SA-2008-10-09 Security Update 2008-007	APPLE
SecurityFocus	BUGTRAQ
Pony Mail!	MLIST
Pony Mail!	MLIST
Security Alerts - Secunia	SECUNIA
SecurityReason - Apache2 CSRF, XSS, Memory Corruption and Denial of Service Vulnerability	SREASON
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:024	SUSE
USN-731-1: Apache vulnerabilities Ubuntu	UBUNTU
Pony Mail!	MLIST
Pony Mail!	
HPSBUX02401	HP
Pony Mail!	MLIST

Pony Mail!	MLIS I
Pony Mail!	MLIST
Repository / Oval Repository	OVAL
Pony Mail!	
Gentoo update for apache - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
Pony Mail!	MLIST
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP Server 2.2.9. http://httpd.apache.org/security/vulnerabilities_22.html
Mandriva	2008-03-12	Vincent Danen	Mandriva ships mod_proxy_balancer but will not be issuing updates to correct this flaw as the
Red Hat	2008-01-24	Mark J Cox	mod_proxy_balancer is shipped in Red Hat Enterprise Linux 5 and Red Hat Application Stack

Legacy QID Mappings	
690551	Free Berkeley Software Distribution (FreeBSD) Security Update for apache (c84dc9ad-41f7-11dd-a4f9-00163e000016)

© [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](#)