



# CVE-2005-2970

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

## Summary

<b>CVE</b>	CVE-2005-2970
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-10-25 17:06:00 UTC
<b>Updated</b>	2023-02-13 01:16:00 UTC
<b>Description</b>	Memory leak in the worker MPM (worker.c) for Apache 2, in certain circumstances, allows remote attackers to cause a deni

## Risk And Classification

**Problem Types:** CWE-770

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.0	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	4.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	5.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	5.10	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora Core</a>	4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	4.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	4.0	All	All	All

## References

Reference	Source	Link
Mailing list archives	MISC	<a href="#">mail-arc</a>

SecurityFocus	FEDORA	<a href="http://www.se">www.se</a>
Pony Mail!	MLIST	<a href="http://lists.apa">lists.apa</a>
[Apache-SVN] Revision 292949	CONFIRM	<a href="http://svn.apa">svn.apa</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>
usn/usn-225-1 - Ubuntu Linux	UBUNTU	<a href="http://www.ub">www.ub</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>
Pony Mail!	MLIST	<a href="http://lists.apa">lists.apa</a>
Secunia - Advisories - Mandriva update for apache2	SECUNIA	<a href="http://secunia">secunia</a>
Secunia - Advisories - Fedora update for httpd	SECUNIA	<a href="http://secunia">secunia</a>
Secunia - Advisories - Ubuntu update for apache2	SECUNIA	<a href="http://secunia">secunia</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>
Pony Mail!	MLIST	<a href="http://lists.apa">lists.apa</a>
<a href="http://rhn.redhat.com">rhn.redhat.com</a>   Red Hat Support	REDHAT	<a href="http://rhn.redh">rhn.redh</a>
Secunia - Advisories - Apache Byte-Range Filter and MPM Worker Denial of Service Vulnerabilities	SECUNIA	<a href="http://secunia">secunia</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cis">oval.cis</a>
Pony Mail!	MLIST	<a href="http://lists.apa">lists.apa</a>
SecurityTracker.com Archives - Apache Memory Leak in MPM 'worker.c' Code May Let Remote Users Deny Service	SECTRACK	<a href="http://security">security</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>
Mailing list archives	CONFIRM	<a href="http://mail-arc">mail-arc</a>
[SECURITY] Fedora Core 4 Update: httpd-2.0.54-10.3	FEDORA	<a href="http://www.re">www.re</a>
Pony Mail!	MLIST	<a href="http://lists.apa">lists.apa</a>
Pony Mail!	MLIST	<a href="http://lists.apa">lists.apa</a>
Security Announcement	SUSE	<a href="http://www.nc">www.nc</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>
Secunia - Advisories - Red Hat update for httpd	SECUNIA	<a href="http://secunia">secunia</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>
Pony Mail!	MLIST	<a href="http://lists.apa">lists.apa</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>
Pony Mail!	MLIST	<a href="http://lists.apa">lists.apa</a>
Advisories - Mandriva Linux	MANDRIVA	<a href="http://www.m:">www.m:</a>
Pony Mail!	MLIST	<a href="http://lists.apa">lists.apa</a>
Apache MPM Worker.C Denial Of Service Vulnerability	BID	<a href="http://www.se">www.se</a>
Pony Mail!	MISC	<a href="http://lists.apa">lists.apa</a>

Pony Mail!	MISC	<a href="#">lists.apa</a>
Pony Mail!	MLIST	<a href="#">lists.apa</a>
Pony Mail!	MISC	<a href="#">lists.apa</a>
Pony Mail!	MLIST	<a href="#">lists.apa</a>
Pony Mail!	MLIST	<a href="#">lists.apa</a>
CVE Program record	CVE.ORG	<a href="#">www.cv</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist</a>

## Vendor Comments And Credit

Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP Server 2.0.55: <a href="http://httpd.apache.org/security/vulnerabilities_20.html">http://httpd.apache.org/security/vulnerabilities_20.html</a>

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)