



# CVE-2010-2791

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2010-2791
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-08-05 18:17:00 UTC
<b>Updated</b>	2023-11-07 02:05:00 UTC
<b>Description</b>	mod_proxy in httpd in Apache HTTP Server 2.2.9, when running on Unix, does not close the backend connection if a timeo

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.9	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.9	All	All	All
Operating System	<a href="#">Unix</a>	<a href="#">Unix</a>	All	All	All	All
Operating System	<a href="#">Unix</a>	<a href="#">Unix</a>	All	All	All	All

## References

Reference	Source	Link
Pony Mail!	MISC	<a href="mailto:lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="mailto:lists.apache.org">lists.apache.org</a>
Oracle Critical Patch Update - April 2013	CONFIRM	<a href="http://www.oracle.com">www.oracle.com</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="mailto:lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="mailto:lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="mailto:lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="mailto:lists.apache.org">lists.apache.org</a>
Apache 'mod_proxy_http' 2.2.9 for Unix Timeout Handling Information Disclosure Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>

oss-security - CVE-2010-2791: mod_proxy information leak affecting 2.2.9 only	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
Pony Mail!	MISC	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="http://lists.apache.org">lists.apache.org</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
Pony Mail!	MISC	<a href="http://lists.apache.org">lists.apache.org</a>
Support / Security / Advisories // MDVSA-2013:150   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>
Pony Mail!	MISC	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Red Hat Customer Portal	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MISC	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="http://lists.apache.org">lists.apache.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

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](https://status.cve.report)**