



# CVE-2014-3583

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

## Summary

<b>CVE</b>	CVE-2014-3583
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-12-15 18:59:00 UTC
<b>Updated</b>	2023-11-07 02:20:00 UTC
<b>Description</b>	The handle_headers function in mod_proxy_fcgi.c in the mod_proxy_fcgi module in the Apache HTTP Server 2.4.10 allows

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.4.10	All	All	All
Application	Apache	Http Server	2.4.10	All	All	All
Operating System	Apple	Mac Os X	10.10.0	All	All	All
Operating System	Apple	Mac Os X	10.10.1	All	All	All
Operating System	Apple	Mac Os X	10.10.2	All	All	All
Operating System	Apple	Mac Os X	10.10.3	All	All	All
Operating System	Apple	Mac Os X	10.10.4	All	All	All
Operating System	Apple	Mac Os X	10.9.5	All	All	All
Operating System	Apple	Mac Os X	10.10.0	All	All	All
Operating System	Apple	Mac Os X	10.10.1	All	All	All
Operating System	Apple	Mac Os X	10.10.2	All	All	All
Operating System	Apple	Mac Os X	10.10.3	All	All	All
Operating System	Apple	Mac Os X	10.10.4	All	All	All
Operating System	Apple	Mac Os X	10.9.5	All	All	All
Operating System	Apple	Os X Server	5.0.3	All	All	All
Operating System	Apple	Os X Server	5.0.3	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All

Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	10.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.10	All	All	All

## References

Reference	Source	Link
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
About the security content of OS X Server v5.0.3 - Apple Support	CONFIRM	<a href="#">support.apple.com</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>
About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006 - Apple Support	CONFIRM	<a href="#">support.apple.com</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Red Hat Customer Portal	REDHAT	<a href="#">rhn.redhat.com</a>
APPLE-SA-2015-09-16-4 OS X Server 5.0.3	APPLE	<a href="#">lists.apple.com</a>
Pony Mail!		<a href="#">lists.apache.org</a>
[Apache-SVN] Revision 1638818	CONFIRM	<a href="#">svn.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
USN-2523-1: Apache HTTP Server vulnerabilities   Ubuntu	UBUNTU	<a href="#">www.ubuntu.com</a>
Bug 1163555 – CVE-2014-3583 httpd: mod_proxy_fcgi handle_headers() buffer over read	CONFIRM	<a href="#">bugzilla.redhat.com</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Pony Mail!	REDHAT	<a href="#">rhn.redhat.com</a>

Hed Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
Apache HTTP Server 'mod_proxy_fcgi' Module Denial of Service Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
APPLE-SA-2015-08-13-2 OS X Yosemite v10.10.5 and Security Update 2015-006	APPLE	<a href="https://lists.apple.com">lists.apple.com</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Apache: Multiple vulnerabilities (GLSA 201701-36) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	CONFIRM	<a href="http://httpd.apache.org">httpd.apache.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Oracle Critical Patch Update - January 2016	CONFIRM	<a href="https://www.oracle.com">www.oracle.com</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

710461 Gentoo Linux Apache Multiple Vulnerabilities (GLSA 201701-36)

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)