



CVE-2014-8109

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

Summary

CVE	CVE-2014-8109
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-29 23:59:00 UTC
Updated	2023-02-13 00:42:00 UTC
Description	mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd cor

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.3.0	All	All	All
Application	Apache	Http Server	2.3.1	All	All	All
Application	Apache	Http Server	2.3.10	All	All	All
Application	Apache	Http Server	2.3.11	All	All	All
Application	Apache	Http Server	2.3.12	All	All	All
Application	Apache	Http Server	2.3.13	All	All	All
Application	Apache	Http Server	2.3.14	All	All	All
Application	Apache	Http Server	2.3.15	All	All	All
Application	Apache	Http Server	2.3.16	All	All	All
Application	Apache	Http Server	2.3.2	All	All	All
Application	Apache	Http Server	2.3.3	All	All	All
Application	Apache	Http Server	2.3.4	All	All	All
Application	Apache	Http Server	2.3.5	All	All	All
Application	Apache	Http Server	2.3.6	All	All	All
Application	Apache	Http Server	2.3.7	All	All	All
Application	Apache	Http Server	2.3.8	All	All	All
Application	Apache	Http Server	2.3.9	All	All	All

Application	Apache	Http Server	2.4.0	All	All	All
Application	Apache	Http Server	2.4.1	All	All	All
Application	Apache	Http Server	2.4.10	All	All	All
Application	Apache	Http Server	2.4.2	All	All	All
Application	Apache	Http Server	2.4.3	All	All	All
Application	Apache	Http Server	2.4.4	All	All	All
Application	Apache	Http Server	2.4.6	All	All	All
Application	Apache	Http Server	2.4.7	All	All	All
Application	Apache	Http Server	2.4.8	All	All	All
Application	Apache	Http Server	2.4.9	All	All	All
Application	Apache	Http Server	2.3.0	All	All	All
Application	Apache	Http Server	2.3.1	All	All	All
Application	Apache	Http Server	2.3.10	All	All	All
Application	Apache	Http Server	2.3.11	All	All	All
Application	Apache	Http Server	2.3.12	All	All	All
Application	Apache	Http Server	2.3.13	All	All	All
Application	Apache	Http Server	2.3.14	All	All	All
Application	Apache	Http Server	2.3.15	All	All	All
Application	Apache	Http Server	2.3.16	All	All	All
Application	Apache	Http Server	2.3.2	All	All	All
Application	Apache	Http Server	2.3.3	All	All	All
Application	Apache	Http Server	2.3.4	All	All	All
Application	Apache	Http Server	2.3.5	All	All	All
Application	Apache	Http Server	2.3.6	All	All	All
Application	Apache	Http Server	2.3.7	All	All	All
Application	Apache	Http Server	2.3.8	All	All	All
Application	Apache	Http Server	2.3.9	All	All	All
Application	Apache	Http Server	2.4.0	All	All	All
Application	Apache	Http Server	2.4.1	All	All	All
Application	Apache	Http Server	2.4.10	All	All	All
Application	Apache	Http Server	2.4.2	All	All	All
Application	Apache	Http Server	2.4.3	All	All	All
Application	Apache	Http Server	2.4.6	All	All	All
Application	Apache	Http Server	2.4.7	All	All	All
Application	Apache	Http Server	2.4.8	All	All	All

Application	Apache	Http Server	2.4.9	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Application	Oracle	Enterprise Manager Ops Center	All	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.2.0	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.2.1	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.3.0	All	All	All

References

Reference	Source	Link
Apache HTTP Server 'mod_lua.c' Local Access Bypass Vulnerability	BID	www.securityfocus.com
Pony Mail!	MLIST	lists.apache.org
About the security content of OS X Server v5.0.3 - Apple Support	CONFIRM	support.apple.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MISC	lists.apache.org
Bug 1174077 – CVE-2014-8109 httpd: LuaAuthzProvider argument handling issue	CONFIRM	bugzilla.redhat.com
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MISC	lists.apache.org
About the security content of OS X Yosemite v10.10.5 and Security Update 2015-006 - Apple Support	CONFIRM	support.apple.com
oss-security - CVE Request: "LuaAuthzProvider" in Apache HTTP Server mixes up arguments	MLIST	www.openwall.com
Pony Mail!	MISC	lists.apache.org
57204 – LuaAuthzProvider mixes up parsed require arguments when used multiple times	CONFIRM	issues.apache.org
Pony Mail!	MISC	lists.apache.org

Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
APPLE-SA-2015-09-16-4 OS X Server 5.0.3	APPLE	lists.apple.com
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
USN-2523-1: Apache HTTP Server vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com
Mageia Advisory: MGASA-2015-0011 - Updated apache packages fix CVE-2014-8109	CONFIRM	advisories.mageia.org
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MISC	lists.apache.org
APPLE-SA-2015-08-13-2 OS X Yosemite v10.10.5 and Security Update 2015-006	APPLE	lists.apple.com
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MISC	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Merge r1642499 from trunk: · apache/httpd@3f1693d · GitHub	CONFIRM	github.com
Pony Mail!	MLIST	lists.apache.org
[SECURITY] Fedora 21 Update: httpd-2.4.12-1.fc21	FEDORA	lists.fedoraproject.org
Pony Mail!	MLIST	lists.apache.org
Oracle Critical Patch Update - January 2016	CONFIRM	www.oracle.com
Pony Mail!	MLIST	lists.apache.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [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/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report