



# CVE-2016-4975

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

## Summary

<b>CVE</b>	CVE-2016-4975
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-08-14 12:29:00 UTC
<b>Updated</b>	2023-11-07 02:32:00 UTC
<b>Description</b>	Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated

## Risk And Classification

### Problem Types: CWE-93

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.0	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.10	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.11	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.12	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.13	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.14	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.15	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.16	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.17	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.18	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.19	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.20	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.21	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.22	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.23	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.24	All	All	All

Application	Apache	Http Server	2.2.25	All	All	All
Application	Apache	Http Server	2.2.26	All	All	All
Application	Apache	Http Server	2.2.27	All	All	All
Application	Apache	Http Server	2.2.29	All	All	All
Application	Apache	Http Server	2.2.3	All	All	All
Application	Apache	Http Server	2.2.31	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	2.2.8	All	All	All
Application	Apache	Http Server	2.2.9	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	2.4.12	All	All	All
Application	Apache	Http Server	2.4.16	All	All	All
Application	Apache	Http Server	2.4.17	All	All	All
Application	Apache	Http Server	2.4.18	All	All	All
Application	Apache	Http Server	2.4.2	All	All	All
Application	Apache	Http Server	2.4.20	All	All	All
Application	Apache	Http Server	2.4.23	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	2.4.9	All	All	All
Application	Apache	Http Server	2.2.0	All	All	All
Application	Apache	Http Server	2.2.10	All	All	All
Application	Apache	Http Server	2.2.11	All	All	All
Application	Apache	Http Server	2.2.12	All	All	All
Application	Apache	Http Server	2.2.13	All	All	All
Application	Apache	Http Server	2.2.14	All	All	All
Application	Apache	Http Server	2.2.15	All	All	All
Application	Apache	Http Server	2.2.16	All	All	All
Application	Apache	Http Server	2.2.17	All	All	All
Application	Apache	Http Server	2.2.18	All	All	All
Application	Apache	Http Server	2.2.19	All	All	All

Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.20	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.21	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.22	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.23	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.24	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.25	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.26	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.27	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.29	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.3	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.31	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.4	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.6	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.2.8	All	All	All
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>	2.4.1	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.10	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.12	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.16	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.17	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.18	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.2	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.20	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.23	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.3	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.4	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.6	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.7	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	2.4.9	All	All	All

## References

Reference	Source	Link	T
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<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>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</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>	
Document Display   HPE Support Center	CONFIRM	<a href="https://support.hpe.com">support.hpe.com</a>	
Pony Mail!		<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>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
httpd 2.2 vulnerabilities - The Apache HTTP Server Project	CONFIRM	<a href="http://httpd.apache.org">httpd.apache.org</a>	V
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</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>	
Malformed Request	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	T
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>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
httpd 2.4 vulnerabilities - The Apache HTTP Server Project	CONFIRM	<a href="http://httpd.apache.org">httpd.apache.org</a>	V
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</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>	
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>	
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>	
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>	
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>	
CVE-2016-4975 Apache HTTP Server Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	T
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>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

### Vendor Comments And Credit

Discovery Credit  
**LEGACY:** The issue was discovered by Sergey Bobrov

### Legacy QID Mappings

- [378182](#) Virtuozzo Linux Security Update for mod\_proxy\_html (VZLSA-2017:0906)
- [730846](#) Apache HTTP Server CRLF Injection Vulnerability (CVE-2016-4975)

© [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](#)