



CVE-2016-8743

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

Summary

CVE	CVE-2016-8743
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-27 21:29:00 UTC
Updated	2023-11-07 02:36:00 UTC
Description	Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and s

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	2.4.1	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	All	All	All	All
Application	Apache	Http Server	All	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Netapp	Oncommand Unified Manager	-	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All

Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Jboss Core Services	1.0	All	All	All

References

Reference
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
About the security content of macOS High Sierra 10.13.1, Security Update 2017-001 Sierra, and Security Update 2017-004 El Capitan - Apple
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
December 2016 Apache HTTP Server Vulnerabilities in Multiple NetApp Products NetApp Product Security
Pony Mail!
Document Display HPE Support Center
Pony Mail!
Debian -- Security Information -- DSA-3796-1 apache2
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!

[R5] SecurityCenter 5.4.3 Fixes Multiple Vulnerabilities - Security Advisory | Tenable Network Security

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Apache HTTPD Multiple Flaws Let Remote Users Deny Service, Conduct HTTP Response Splitting Attacks, and Access and Modify Session I

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Document Display | HPE Support Center

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Red Hat Customer Portal

Pony Mail!

Pony Mail!

Apache HTTP Server CVE-2016-8743 Security Bypass Vulnerability

httpd 2.4 vulnerabilities - The Apache HTTP Server Project

Pony Mail!

Apache: Multiple vulnerabilities (GLSA 201701-36) — Gentoo security

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

CVE Program record

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378176](#) Virtuozzo Linux Security Update for mod_ssl (VZLSA-2017:1721)

[378182](#) Virtuozzo Linux Security Update for mod_proxy_html (VZLSA-2017:0906)

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

© [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](#)