



CVE-2017-7668

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

Summary

CVE	CVE-2017-7668
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-20 01:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allo

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.2.0	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	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.20	All	All	All
Application	Apache	Http Server	2.2.21	All	All	All
Application	Apache	Http Server	2.2.22	All	All	All
Application	Apache	Http Server	2.2.23	All	All	All
Application	Apache	Http Server	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	2.2.30	All	All	All
Application	Apache	Http Server	2.2.31	All	All	All
Application	Apache	Http Server	2.2.32	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	2.4.24	All	All	All
Application	Apache	Http Server	2.4.25	All	All	All
Application	Apache	Http Server	2.2.0	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	Apache	Http Server	2.2.2	All	All	All
Application	Apache	Http Server	2.2.20	All	All	All
Application	Apache	Http Server	2.2.21	All	All	All
Application	Apache	Http Server	2.2.22	All	All	All
Application	Apache	Http Server	2.2.23	All	All	All
Application	Apache	Http Server	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	2.2.30	All	All	All
Application	Apache	Http Server	2.2.31	All	All	All
Application	Apache	Http Server	2.2.32	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	2.4.25	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	10.11.6	-	All	All
Operating System	Apple	Mac Os X	10.11.6	security_update_2016-001	All	All
Operating System	Apple	Mac Os X	10.11.6	security_update_2016-002	All	All
Operating System	Apple	Mac Os X	10.11.6	security_update_2016-003	All	All
Operating System	Apple	Mac Os X	10.11.6	security_update_2017-001	All	All
Operating System	Apple	Mac Os X	10.11.6	security_update_2017-002	All	All
Operating System	Apple	Mac Os X	10.11.6	security_update_2017-003	All	All
Operating System	Apple	Mac Os X	10.12.6	-	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
Application	Netapp	Storagegrid	-	All	All	All
Application	Oracle	Secure Global Desktop	5.3	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.2	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	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	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	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	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	7.0	All	All	All

References

Reference

Debian -- Security Information -- DSA-3896-1 apache2

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Pony Mail!

Red Hat Customer Portal

Document Display | HPE Support Center

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!

Pony Mail!

Pony Mail!

Apache HTTPD Bugs Let Remote Users Deny Service and Bypass Authentication in Certain Cases - SecurityTracker

Pony Mail!

Red Hat Customer Portal

Pony Mail!
Pony Mail!
Document Display HPE Support Center
Pony Mail!
[R1] Tenable.sc 5.13.0 Fixes Multiple Third-Party Vulnerabilities - Security Advisory Tenable®
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Apache HTTP Server CVE-2017-7668 Denial of Service Vulnerability
Pony Mail!
Pony Mail!
Red Hat Customer Portal
June 2017 Apache HTTP Server Vulnerabilities in NetApp Products NetApp Product Security
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Apache: Multiple vulnerabilities (GLSA 201710-32) — Gentoo security
Pony Mail!
Pony Mail!
Pony Mail!
Oracle Critical Patch Update - October 2017
Pony Mail!
Pony Mail!

Pony mail!

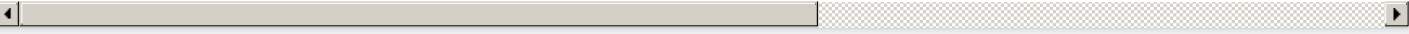
Pony Mail!

Pony Mail!

Pony Mail!

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500011](#) Alpine Linux Security Update for apache2

[503702](#) Alpine Linux Security Update for apache2

© [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](#)