



CVE-2018-17189

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

Summary

CVE	CVE-2018-17189
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-30 22:29:00 UTC
Updated	2023-11-07 02:54:00 UTC
Description	In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 s

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	2.4.17	All	All	All
Application	Apache	Http Server	2.4.18	All	All	All
Application	Apache	Http Server	2.4.20	All	All	All
Application	Apache	Http Server	2.4.23	All	All	All
Application	Apache	Http Server	2.4.25	All	All	All
Application	Apache	Http Server	2.4.26	All	All	All
Application	Apache	Http Server	2.4.27	All	All	All
Application	Apache	Http Server	2.4.28	All	All	All
Application	Apache	Http Server	2.4.29	All	All	All
Application	Apache	Http Server	2.4.30	All	All	All
Application	Apache	Http Server	2.4.33	All	All	All
Application	Apache	Http Server	2.4.34	All	All	All
Application	Apache	Http Server	2.4.35	All	All	All
Application	Apache	Http Server	2.4.37	All	All	All
Application	Apache	Http Server	All	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All

Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Application	Netapp	Santricity Cloud Connector	-	All	All	All
Application	Netapp	Santricity Cloud Connector	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.3.3	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.3.3	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.0	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.2	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.3	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.0	All	All	All
Application	Oracle	Retail Xstore Point Of Service	7.1	All	All	All
Application	Oracle	Sun Zfs Storage Appliance Kit	8.8.6	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Jboss Core Services	1.0	All	All	All

References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	access.redhat.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Debian -- Security Information -- DSA-4422-1 apache2	DEBIAN	www.debian.org
Pony Mail!		lists.apache.org

Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Bugtraq: [SECURITY] [DSA 4422-1] apache2 security update	BUGTRAQ	seclists.org
Pony Mail!		lists.apache.org
USN-3937-1: Apache HTTP Server vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
Apache HTTP Server CVE-2018-17189 Denial of Service Vulnerability	BID	www.securityfocus.com
[R1] Tenable.sc 5.13.0 Fixes Multiple Third-Party Vulnerabilities - Security Advisory Tenable®	CONFIRM	www.tenable.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
January 2019 Apache HTTP Server Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
Pony Mail!	MLIST	lists.apache.org
[SECURITY] Fedora 28 Update: mod_http2-1.14.1-1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
Apache: Multiple vulnerabilities (GLSA 201903-21) — Gentoo security	GENTOO	security.gentoo.org
Pony Mail!		lists.apache.org
[SECURITY] Fedora 29 Update: mod_http2-1.14.1-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 29 Update: mod_http2-1.14.1-1.fc29 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Document Display HPE Support Center	CONFIRM	support.hpe.com
Oracle Critical Patch Update - July 2019	MISC	www.oracle.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
[SECURITY] Fedora 28 Update: mod_http2-1.14.1-1.fc28 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	CONFIRM	httpd.apache.org
Pony Mail!	MLIST	lists.apache.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Pony Mail!	MLIST	lists.apache.org
Oracle Critical Patch Update Advisory - January 2020	MISC	www.oracle.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Pony Mail!	MLIST	lists.apache.org

Oracle Critical Patch Update Advisory - April 2019	MISC	www.oracle.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296087](#) Oracle Solaris 11.4 Support Repository Update (SRU) 8.1.5 Missing (CPUAPR2019)

[500016](#) Alpine Linux Security Update for apache2

[503707](#) Alpine Linux Security Update for apache2

[710186](#) Gentoo Linux Apache Multiple vulnerabilities (GLSA 201903-21)

[940248](#) AlmaLinux Security Update for httpd:2.4 (ALSA-2020:4751)

[960434](#) Rocky Linux Security Update for httpd:2.4 (RLSA-2020:4751)

© [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](#)