



# CVE-2019-0196

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

## Summary

<b>CVE</b>	CVE-2019-0196
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-06-11 22:29:00 UTC
<b>Updated</b>	2023-11-07 03:01:00 UTC
<b>Description</b>	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Http Server</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All

## References

Reference	Source	Link
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</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>
<a href="https://support.f5.com/csp/article/K44591505">support.f5.com/csp/article/K44591505</a>	CONFIRM	<a href="https://support.f5.com">support.f5.com</a>
Debian -- Security Information -- DSA-4422-1 apache2	DEBIAN	<a href="http://www.debian.org">www.debian.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>
Bugtraq: [SECURITY] [DSA 4422-1] apache2 security update	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
USN-3937-1: Apache HTTP Server vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
[SECURITY] Fedora 30 Update: mod_http2-1.15.0-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.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>
[SECURITY] Fedora 30 Update: httpd-2.4.39-2.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
[security-announce] openSUSE-SU-2019:1209-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
[SECURITY] Fedora 30 Update: httpd-2.4.39-2.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
404 Not Found	MISC	<a href="http://www.apache.org">www.apache.org</a>
June 2019 Apache HTTP Server Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</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!		<a href="https://lists.apache.org">lists.apache.org</a>
[SECURITY] Fedora 29 Update: mod_http2-1.15.1-1.fc29 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Apache httpd CVE-2019-0196 Security Bypass Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
Document Display   HPE Support Center	CONFIRM	<a href="https://support.hpe.com">support.hpe.com</a>
oss-security - CVE-2019-0196: mod_http2, read-after-free on a string compare	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>
Oracle Critical Patch Update - July 2019	MISC	<a href="https://www.oracle.com">www.oracle.com</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
[security-announce] openSUSE-SU-2019:1258-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	CONFIRM	<a href="https://httpd.apache.org">httpd.apache.org</a>
[SECURITY] Fedora 30 Update: mod_http2-1.15.1-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>

[SECURITY] Fedora 29 Update: mod_http2-1.15.1-1.fc29 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Oracle Critical Patch Update - October 2019	MISC	<a href="https://www.oracle.com">www.oracle.com</a>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Oracle Critical Patch Update Advisory - April 2020	N/A	<a href="https://www.oracle.com">www.oracle.com</a>
[SECURITY] Fedora 30 Update: mod_http2-1.15.0-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.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>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</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>
[security-announce] openSUSE-SU-2019:1190-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

[377378](#) Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2022:0017)

[500017](#) Alpine Linux Security Update for apache2

[503708](#) Alpine Linux Security Update for apache2

[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](https://status.cve.report)