



# CVE-2019-0211

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-0211
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-04-08 22:29:00 UTC
<b>Updated</b>	2023-11-07 03:01:00 UTC
<b>Description</b>	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged

## Risk And Classification

**EPSS:** 0.901590000 probability, percentile 0.995860000 (date 2026-04-01)

**CISA KEV:** Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

**Problem Types:** CWE-416

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Apache
<b>Product</b>	HTTP Server
<b>Name</b>	Apache HTTP Server Privilege Escalation Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2019-0211">https://nvd.nist.gov/vuln/detail/CVE-2019-0211</a>

## 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
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All

## References

Reference	Source	Link
Slackware Security Advisory - httpd Updates ≈ Packet Storm	MISC	<a href="#">packetstormsecurity</a>
Pony Mail!		<a href="#">lists.apache.org</a>
[SECURITY] Fedora 28 Update: httpd-2.4.39-1.1.fc28 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.or</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Synology Inc.	CONFIRM	<a href="#">www.synology.com</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Red Hat Customer Portal	REDHAT	<a href="#">access.redhat.com</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
<a href="#">support.f5.com/csp/article/K32957101</a>	CONFIRM	<a href="#">support.f5.com</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Debian -- Security Information -- DSA-4422-1 apache2	DEBIAN	<a href="#">www.debian.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Bugtraq: [SECURITY] [DSA 4422-1] apache2 security update	BUGTRAQ	<a href="#">seclists.org</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>
USN-3937-1: Apache HTTP Server vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.ubuntu.com</a>
Pony Mail!	MLIST	<a href="#">lists.apache.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>
Pony Mail!		<a href="#">lists.apache.org</a>

Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation - Linux local Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</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>
[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>
Apache 2.4.38 Root Privilege Escalation ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity</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>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
[SECURITY] Fedora 29 Update: httpd-2.4.39-2.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>
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>
[SECURITY] Fedora 29 Update: httpd-2.4.39-2.fc29 - 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>
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>
Document Display   HPE Support Center	CONFIRM	<a href="https://support.hpe.com">support.hpe.com</a>
Oracle Critical Patch Update - July 2019	MISC	<a href="http://www.oracle.com">www.oracle.com</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	MISC	<a href="http://httpd.apache.org">httpd.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!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
April 2019 Apache HTTP Server Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
[security-announce] openSUSE-SU-2019:1258-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Apache HTTP Server CVE-2019-0211 Local Privilege Escalation Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
[SECURITY] Fedora 28 Update: httpd-2.4.39-1.1.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
oss-security - Re: Statistics for distros lists updated for 2019Q2	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
Apache: Privilege escalation (GLSA 201904-20) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
oss-security - CVE-2019-0211: Apache HTTP Server privilege escalation from modules' scripts	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>
Bugtraq: [slackware-security] httpd (SSA:2019-096-01)	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>

Pony Mail!		<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>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
Oracle Critical Patch Update Advisory - April 2020	N/A	<a href="https://www.oracle.com">www.oracle.com</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>
CARPE (DIEM) Apache 2.4.x Local Privilege Escalation ≈ Packet Storm	MISC	<a href="https://packetstormsecurity">packetstormsecurity</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>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</a>
[security-announce] openSUSE-SU-2019:1190-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.com</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>
CISA Known Exploited Vulnerabilities catalog	CISA	<a href="https://www.cisa.gov">www.cisa.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

[710165](#) Gentoo Linux Apache Privilege escalation Vulnerability (GLSA 201904-20)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)