



CVE-2018-17199

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-17199 |
| 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 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the ses |

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|--|---------|--------|---------|----------|
| 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 | 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 | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | 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 | 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 |

References

| Reference | Source | Link | T |
|--|---------|---|----|
| 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! | MLIST | lists.apache.org | |
| Pony Mail! | | lists.apache.org | |
| Debian -- Security Information -- DSA-4422-1 apache2 | DEBIAN | www.debian.org | T |
| 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 | Is |
| [SECURITY] [DLA 1647-1] apache2 security update | MLIST | lists.debian.org | M |
| Pony Mail! | | lists.apache.org | |
| USN-3937-1: Apache HTTP Server vulnerabilities Ubuntu security notices | UBUNTU | usn.ubuntu.com | T |
| Pony Mail! | | lists.apache.org | |
| [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 | T |
| Pony Mail! | MLIST | lists.apache.org | |
| Apache: Multiple vulnerabilities (GLSA 201903-21) — Gentoo security | GENTOO | security.gentoo.org | T |
| Pony Mail! | | lists.apache.org | |
| Document Display HPE Support Center | CONFIRM | support.hpe.com | |
| Oracle Critical Patch Update - July 2019 | MISC | www.oracle.com | |
| Pony Mail! | MLIST | lists.apache.org | |
| Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project | CONFIRM | httpd.apache.org | V |
| Pony Mail! | MLIST | lists.apache.org | |
| Pony Mail! | REDHAT | access.redhat.com | |

| | | | |
|---|---------|---|----|
| Hed Hat Customer Portal | REDHAT | access.redhat.com | |
| Red Hat Customer Portal | REDHAT | access.redhat.com | |
| Pony Mail! | MLIST | lists.apache.org | |
| Pony Mail! | | 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 | |
| Apache HTTP Server CVE-2018-17199 Remote Security Vulnerability | BID | www.securityfocus.com | T |
| Oracle Critical Patch Update Advisory - April 2019 | MISC | www.oracle.com | P |
| CVE Program record | CVE.ORG | www.cve.org | ca |
| NVD vulnerability detail | NVD | nvd.nist.gov | ca |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159218](#) Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2021-1809)

[239299](#) Red Hat Update for httpd:2.4 (RHSA-2021:1809)

[377287](#) Alibaba Cloud Linux Security Update for httpd (ALINUX2-SA-2020:0075)

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

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

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

[87456](#) IBM HTTP Server Multiple Vulnerabilities(6467651,869064)

[940395](#) AlmaLinux Security Update for httpd:2.4 (ALSA-2021:1809)

[960396](#) Rocky Linux Security Update for httpd:2.4 (RLSA-2021:1809)

© 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