# CVE-2019-10092

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2019-10092 |
| **State** | PUBLIC |
| **Assigner** | security@apache.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2019-09-26 16:15:00 UTC |
| **Updated** | 2023-11-07 03:02:00 UTC |
| **Description** | In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. A |

## Risk And Classification

**Problem Types:** CWE-79

## 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 | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 19.04 | 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 | 19.04 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | 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 | 10.0 | 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 | Fedoraproject | Fedora | 30 | All | All | All |
| Operating System | Fedoraproject | Fedora | 30 | All | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | - | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | p1 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Netapp | Clustered Data Ontap | 9.6 | p3 | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | p4 | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | p7 | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | p8 | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | - | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | p1 | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | p3 | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | p4 | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | p7 | All | All |
| Operating System | Netapp | Clustered Data Ontap | 9.6 | p8 | All | All |
| Operating System | Netapp | Clustered Data Ontap | All | All | All | All |
| Operating System | Opensuse | Leap | 15.0 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Operating System | Opensuse | Leap | 15.0 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Application | Oracle | Communications Element Manage | 8.0.0 | All | All | All |
| Application | Oracle | Communications Element Manage | 8.1.0 | All | All | All |
| Application | Oracle | Communications Element Manage | 8.1.1 | All | All | All |
| Application | Oracle | Communications Element Manage | 8.2.0 | All | All | All |
| Application | Oracle | Communications Element Manage | 8.0.0 | All | All | All |
| Application | Oracle | Communications Element Manage | 8.1.0 | All | All | All |
| Application | Oracle | Communications Element Manage | 8.1.1 | All | All | All |
| Application | Oracle | Communications Element Manage | 8.2.0 | All | All | All |
| Application | Oracle | Communications Element Manager | 8.0.0 | All | All | All |
| Application | Oracle | Communications Element Manager | 8.1.0 | All | All | All |
| Application | Oracle | Communications Element Manager | 8.1.1 | All | All | All |
| Application | Oracle | Communications Element Manager | 8.2.0 | All | All | All |
| Application | Oracle | Enterprise Manager Ops Center | 12.3.3 | All | All | All |
| Application | Oracle | Enterprise Manager Ops Center | 12.4.0 | All | All | All |
| Application | Oracle | Enterprise Manager Ops Center | 12.3.3 | All | All | All |
| Application | Oracle | Enterprise Manager Ops Center | 12.4.0 | All | All | All |
| Application | Oracle | Secure Global Desktop | 5.4 | All | All | All |
| Application | Oracle | Secure Global Desktop | 5.5 | All | All | All |
| Application | Oracle | Secure Global Desktop | 5.4 | All | All | All |
| Application | Oracle | Secure Global Desktop | 5.5 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Redhat | Software Collection | 1.0 | All | All | All |
| Application | Redhat | Software Collection | 1.0 | All | All | All |

## References

| Reference |
|---|
| Pony Mail! |
| [SECURITY] [DLA 1900-2] apache2 regression update |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Debian -- Security Information -- DSA-4509-1 apache2 |
| oss-security - Re: CVE-2020-11984: Apache httpd: mod_uwsgi buffer overlow |
| Pony Mail! |
| Pony Mail! |
| September 2019 Apache HTTP Server Vulnerabilities in NetApp Products \| NetApp Product Security |
| Oracle Critical Patch Update Advisory - July 2020 |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| oss-security - CVE-2019-10092: Limited cross-site scripting in mod_proxy |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Oracle Critical Patch Update - October 2019 |
| Pony Mail! |
| USN-4113-1: Apache HTTP Server vulnerabilities \| Ubuntu security notices \| Ubuntu |
| oss-security - Re: CVE-2020-11984: Apache httpd: mod_uwsgi buffer overlow |
| Pony Mail! |
| support.f5.com/csp/article/K30442259 |
| Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project |
| [SECURITY] [DLA 1900-1] apache2 security update |
| Pony Mail! |

| |
|---|
| Pony Mail! |
| Apache: Multiple vulnerabilities (GLSA 201909-04) — Gentoo security |
| Red Hat Customer Portal |
| Bugtraq: [SECURITY] [DSA 4509-3] apache2 security update |
| Pony Mail! |
| [SECURITY] Fedora 30 Update: httpd-2.4.41-1.fc30 - package-announce - Fedora Mailing-Lists |
| Oracle Critical Patch Update Advisory - January 2020 |
| Pony Mail! |
| Oracle Critical Patch Update Advisory - April 2020 |
| [SECURITY] Fedora 30 Update: httpd-2.4.41-1.fc30 - package-announce - Fedora Mailing-Lists |
| Disclosures/CVE-2019-10092-Limited Cross-Site Scripting in mod_proxy Error Page-Apache httpd at master · DrunkenShells/Disclosures · Git |
| Pony Mail! |
| Pony Mail! |
| Bugtraq: [SECURITY] [DSA 4509-1] apache2 security update |
| [security-announce] openSUSE-SU-2019:2051-1: important: Security update |
| Pony Mail! |
| Pony Mail! |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 376862 IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (964768)
- 377378 Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2022:0017)
- 500018 Alpine Linux Security Update for apache2
- 503709 Alpine Linux Security Update for apache2
- 710128 Gentoo Linux Apache Multiple vulnerabilities (GLSA 201909-04)
- 750660 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2021:2004-1)
- 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 registred 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**