



CVE-2020-11984

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

Summary

CVE	CVE-2020-11984
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-07 16:15:00 UTC
Updated	2023-11-07 03:15:00 UTC
Description	Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE

Risk And Classification

Problem Types: CWE-120

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	20.04	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	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	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	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All

Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Oracle	Communications Element Manager	All	All	All	All
Application	Oracle	Communications Session Report Manager	All	All	All	All
Application	Oracle	Communications Session Route Manager	All	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.4.0.0	All	All	All
Application	Oracle	Enterprise Manager Ops Center	12.4.0.0	All	All	All
Application	Oracle	Hyperion Infrastructure Technology	11.1.2.4	All	All	All
Application	Oracle	Hyperion Infrastructure Technology	11.1.2.4	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	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	Zfs Storage Appliance Kit	8.8	All	All	All
Application	Oracle	Zfs Storage Appliance Kit	8.8	All	All	All

References

Reference	Source	Link
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
[security-announce] openSUSE-SU-2020:1285-1: moderate: Security update f	SUSE	lists.opensuse.org
Pony Mail!	MLIST	lists.apache.org
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!	MLIST	lists.apache.org
Debian -- Security Information -- DSA-4757-1 apache2	DEBIAN	www.debian.org
oss-security - Re: CVE-2020-11984: Apache httpd: mod_uwsgi buffer overflow	MLIST	www.openwall.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org

Pony Mail!		lists.apache.org
[SECURITY] [DLA 2362-1] uwsgi security update	MLIST	lists.debian.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
[SECURITY] Fedora 32 Update: httpd-2.4.46-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
August 2020 Apache HTTP Server Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
oss-security - Re: CVE-2020-11984: Apache httpd: mod_uwsgi buffer overflow	MLIST	www.openwall.com
Pony Mail!		lists.apache.org
oss-security - Re: CVE-2020-11984: Apache httpd: mod_uwsgi buffer overflow	MLIST	www.openwall.com
[security-announce] openSUSE-SU-2020:1293-1: moderate: Security update f	SUSE	lists.opensuse.org
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	MISC	httpd.apache.org
oss-security - Re: CVE-2020-11984: Apache httpd: mod_uwsgi buffer overflow	MLIST	www.openwall.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
[SECURITY] Fedora 31 Update: httpd-2.4.46-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Pony Mail!	MLIST	lists.apache.org
Apache: Multiple vulnerabilities (GLSA 202008-04) — Gentoo security	GENTOO	security.gentoo.org
oss-security - Re: CVE-2020-11984: Apache httpd: mod_uwsgi buffer overflow	MLIST	www.openwall.com
Apache2 mod_proxy_uwsgi Incorrect Request Handling ≈ Packet Storm	MISC	packetstormsecurity.com
[httpd-cvs] 20210330 svn commit: r1888199 - /httpd/site/trunk/content/security/vulnerabilities-httpd.xml		lists.apache.org
[SECURITY] Fedora 32 Update: httpd-2.4.46-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
oss-security - Re: CVE-2020-11984: Apache httpd: mod_uwsgi buffer overflow	MLIST	www.openwall.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
USN-4458-1: Apache HTTP Server vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
Oracle Critical Patch Update Advisory - January 2021	MISC	www.oracle.com
[SECURITY] Fedora 31 Update: httpd-2.4.46-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
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

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

[198476](#) Ubuntu Security Notification for uWSGI Vulnerability (USN-5054-1)

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

[296072](#) Oracle Solaris 11.4 Support Repository Update (SRU) 25.75.3 Missing (CPUJUL2020)

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

[500020](#) Alpine Linux Security Update for apache2

[503711](#) Alpine Linux Security Update for apache2

[690506](#) Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (76700d2f-d959-11ea-b53c-d4c9ef517024)

[900119](#) CBL-Mariner Linux Security Update for httpd 2.4.43

[902803](#) Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (1975)

[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](#)