



# CVE-2021-44790

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

## Summary

<b>CVE</b>	CVE-2021-44790
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-12-20 12:15:00 UTC
<b>Updated</b>	2023-11-07 03:39:00 UTC
<b>Description</b>	A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody()) called from Lua

## Risk And Classification

**Problem Types:** CWE-787

## 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="#">Apple</a>	<a href="#">Macos</a>	All	All	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2020-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2021-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2021-002	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2021-003	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2021-004	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2021-005	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2021-006	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2021-007	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2021-008	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2022-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2022-002	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Macos</a>	10.15.7	security_update_2022-003	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2020-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2021-001	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	security_update_2021-002	All	All

Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	<a href="#">security_update_2021-003</a>	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	<a href="#">security_update_2021-004</a>	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	<a href="#">security_update_2021-005</a>	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	<a href="#">security_update_2021-006</a>	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	<a href="#">security_update_2021-007</a>	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	<a href="#">security_update_2021-008</a>	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	<a href="#">security_update_2022-001</a>	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	<a href="#">security_update_2022-002</a>	All	All
Operating System	<a href="#">Apple</a>	<a href="#">Mac Os X</a>	10.15.7	<a href="#">security_update_2022-003</a>	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	36	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Element Manager</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Operations Monitor</a>	4.3	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Operations Monitor</a>	4.4	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Operations Monitor</a>	5.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Session Report Manager</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Session Route Manager</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Http Server</a>	12.2.1.3.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Http Server</a>	12.2.1.4.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Instantis Enterprisetrack</a>	17.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Instantis Enterprisetrack</a>	17.2	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Instantis Enterprisetrack</a>	17.3	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Zfs Storage Appliance Kit</a>	8.8	All	All	All
Application	<a href="#">Tenable</a>	<a href="#">Tenable.sc</a>	All	All	All	All

## References

### Reference

[Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project](#)

[Apache HTTPD: Multiple Vulnerabilities \(GLSA 202208-20\) — Gentoo security](#)

[\[SECURITY\] Fedora 36 Update: httpd-2.4.53-1.fc36 - package-announce - Fedora Mailing-Lists](#)

[About the security content of macOS Big Sur 11.6.6 - Apple Support](#)

Full Disclosure: APPLE-SA-2022-05-16-2 macOS Monterey 12.4

About the security content of macOS Monterey 12.4 - Apple Support

oss-security - CVE-2021-44790: Apache HTTP Server: Possible buffer overflow when parsing multipart content in mod\_lua of Apache HTTP S

[R1] Tenable.sc 5.20.0 Fixes Multiple Vulnerabilities - Security Advisory | Tenable®

Oracle Critical Patch Update Advisory - April 2022

[SECURITY] Fedora 34 Update: httpd-2.4.53-1.fc34 - package-announce - Fedora Mailing-Lists

Apache 2.4.x Buffer Overflow ≈ Packet Storm

Debian -- Security Information -- DSA-5035-1 apache2

About the security content of Security Update 2022-004 Catalina - Apple Support

[SECURITY] Fedora 35 Update: httpd-2.4.53-1.fc35 - package-announce - Fedora Mailing-Lists

[R1] Stand-alone Security Patch Available for Tenable.sc versions 5.16.0 to 5.19.1: Patch 202201.1 - Security Advisory | Tenable®

Oracle Critical Patch Update Advisory - January 2022

[SECURITY] Fedora 36 Update: httpd-2.4.53-1.fc36 - package-announce - Fedora Mailing-Lists

Full Disclosure: APPLE-SA-2022-05-16-3 macOS Big Sur 11.6.6

[SECURITY] Fedora 34 Update: httpd-2.4.53-1.fc34 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 35 Update: httpd-2.4.52-1.fc35 - package-announce - Fedora Mailing-Lists

Full Disclosure: APPLE-SA-2022-05-16-4 Security Update 2022-004 Catalina

[SECURITY] Fedora 35 Update: httpd-2.4.53-1.fc35 - package-announce - Fedora Mailing-Lists

December 2021 Apache HTTP Server Vulnerabilities in NetApp Products | NetApp Product Security

[SECURITY] Fedora 35 Update: httpd-2.4.52-1.fc35 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Chamal

**LEGACY:** Anonymous working with Trend Micro Zero Day Initiative

## Legacy QID Mappings

[150462](#) Apache HTTP Server Buffer Overflow Vulnerability (CVE-2021-44790)

[159594](#) Oracle Enterprise Linux Security Update for httpd (ELSA-2022-0143)

[159602](#) Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-0258)

[178985](#) Debian Security Update for apache2 (DSA 5035-1)

[179048](#) Debian Security Update for apache2 (DLA 2907-1)

184936 Debian Security Update for apache2 (CVE-2021-44790)
198620 Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-5212-1)
240007 Red Hat Update for httpd (RHSA-2022:0143)
240038 Red Hat Update for httpd:2.4 (RHSA-2022:0258)
240041 Red Hat Update for httpd24-httpd (RHSA-2022:0303)
240426 Red Hat Update for httpd:2.4 (RHSA-2022:0288)
257148 CentOS Security Update for httpd (CESA-2022:0143)
282186 Fedora Security Update for httpd (FEDORA-2021-29a536c2ae)
282500 Fedora Security Update for httpd (FEDORA-2022-b4103753e9)
282521 Fedora Security Update for httpd (FEDORA-2022-21264ec6db)
296061 Oracle Solaris 11.4 Support Repository Update (SRU) 42.113.1 Missing (CPUJAN2022)
353114 Amazon Linux Security Advisory for httpd24 : ALAS-2022-1560
353126 Amazon Linux Security Advisory for httpd : ALAS2-2022-1737
354343 Amazon Linux Security Advisory for httpd : ALAS2022-2022-018
354482 Amazon Linux Security Advisory for httpd : ALAS2022-2022-202
354577 Amazon Linux Security Advisory for httpd : ALAS2022-2022-202
355264 Amazon Linux Security Advisory for httpd : ALAS2023-2023-072
376607 Apple macOS Security Update 2022-004 Catalina (HT213255)
376608 Apple MacOS Big Sur 11.6.6 Not Installed (HT213256)
376612 Apple macOS Monterey 12.4 Not Installed (HT213257)
377218 Alibaba Cloud Linux Security Update for httpd (ALINUX2-SA-2022:0004)
377378 Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2022:0017)
378371 IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6540288)
500025 Alpine Linux Security Update for apache2
503716 Alpine Linux Security Update for apache2
590870 Mitsubishi Electric MELSOFT iQ AppPortal Multiple Vulnerabilities (ICSA-22-132-02)
671368 EulerOS Security Update for httpd (EulerOS-SA-2022-1306)
671389 EulerOS Security Update for httpd (EulerOS-SA-2022-1290)

671402 EulerOS Security Update for httpd (EulerOS-SA-2022-1326)
671419 EulerOS Security Update for httpd (EulerOS-SA-2022-1349)
671509 EulerOS Security Update for httpd (EulerOS-SA-2022-1488)
671515 EulerOS Security Update for httpd (EulerOS-SA-2022-1507)
671659 EulerOS Security Update for httpd (EulerOS-SA-2022-1730)
690751 Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (ca982e2d-61a9-11ec-8be6-d4c9ef517024)
710595 Gentoo Linux Apache HTTPD Multiple Vulnerabilities (GLSA 202208-20)
730312 Apache Hypertext Transfer Protocol (HTTP) Server Buffer Overflow Vulnerability
751596 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0065-1)
751604 OpenSUSE Security Update for apache2 (openSUSE-SU-2022:0091-1)
751606 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0119-1)
751711 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0440-1)
752001 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0091-1)
753104 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0091-2)
900337 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (7035)
901425 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (7044-1)
940438 AlmaLinux Security Update for httpd:2.4 (ALSA-2022:0258)
960730 Rocky Linux Security Update for httpd:2.4 (RLSA-2022:0258)

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)