



# CVE-2022-22719

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

## Summary

<b>CVE</b>	CVE-2022-22719
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-03-14 11:15:00 UTC
<b>Updated</b>	2023-11-07 03:43:00 UTC
<b>Description</b>	A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This i

## Risk And Classification

**Problem Types:** CWE-665

## 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	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	All	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	Apple	Mac Os X	10.15.7	security_update_2021-001	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-002	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-003	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-004	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-005	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-006	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-007	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-008	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2022-001	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2022-002	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2022-003	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Oracle	Http Server	12.2.1.3.0	All	All	All
Application	Oracle	Http Server	12.2.1.4.0	All	All	All
Application	Oracle	Zfs Storage Appliance Kit	8.8	All	All	All

## References

Reference	Source	Link
Apache HTTPD: Multiple Vulnerabilities (GLSA 202208-20) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
[SECURITY] Fedora 36 Update: httpd-2.4.53-1.fc36 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
About the security content of macOS Big Sur 11.6.6 - Apple Support	CONFIRM	<a href="https://support.apple.com">support.apple.com</a>
Full Disclosure: APPLE-SA-2022-05-16-2 macOS Monterey 12.4	FULLDISC	<a href="https://seclists.org">seclists.org</a>
About the security content of macOS Monterey 12.4 - Apple Support	CONFIRM	<a href="https://support.apple.com">support.apple.com</a>
Oracle Critical Patch Update Advisory - April 2022	MISC	<a href="https://www.oracle.com">www.oracle.com</a>
[SECURITY] [DLA 2960-1] apache2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] Fedora 34 Update: httpd-2.4.53-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
About the security content of Security Update 2022-004 Catalina - Apple Support	CONFIRM	<a href="https://support.apple.com">support.apple.com</a>
[SECURITY] Fedora 35 Update: httpd-2.4.53-1.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
March 2022 Apache HTTP Server Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	MISC	<a href="https://httpd.apache.org">httpd.apache.org</a>
[SECURITY] Fedora 36 Update: httpd-2.4.53-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
oss-security - CVE-2022-22719: Apache HTTP Server: mod_lua Use of uninitialized value of in r:parsebody	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>
Full Disclosure: APPLE-SA-2022-05-16-2 macOS Monterey 12.4	FULLDISC	<a href="https://seclists.org">seclists.org</a>

Full Disclosure: APPLE-SA-2022-05-16-3 macOS Big Sur 11.6.6	FULLDISC	<a href="https://seclists.org">seclists.org</a>
[SECURITY] Fedora 34 Update: httpd-2.4.53-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject</a>
Full Disclosure: APPLE-SA-2022-05-16-4 Security Update 2022-004 Catalina	FULLDISC	<a href="https://seclists.org">seclists.org</a>
[SECURITY] Fedora 35 Update: httpd-2.4.53-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject</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>

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Chamal De Silva

## Legacy QID Mappings

- 150515 Apache HTTP Server 2.4.53 Multiple Vulnerabilities
- 160250 Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-7647)
- 160309 Oracle Enterprise Linux Security Update for httpd (ELSA-2022-8067)
- 179151 Debian Security Update for apache2 (DLA 2960-1)
- 179224 Debian Security Update for apache2 (CVE-2022-22719)
- 198705 Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-5333-1)
- 240698 Red Hat Update for httpd24-httpd (RHSA-2022:6753)
- 240854 Red Hat Update for httpd:2.4 (RHSA-2022:7647)
- 240885 Red Hat Update for httpd security (RHSA-2022:8067)
- 282500 Fedora Security Update for httpd (FEDORA-2022-b4103753e9)
- 282521 Fedora Security Update for httpd (FEDORA-2022-21264ec6db)
- 296057 Oracle Solaris 11.4 Support Repository Update (SRU) 44.113.4 Missing (bulletinapr2022)
- 353269 Amazon Linux Security Advisory for httpd : ALAS2-2022-1783
- 353274 Amazon Linux Security Advisory for httpd24 : ALAS-2022-1584
- 354481 Amazon Linux Security Advisory for httpd : ALAS2022-2022-053
- 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)

<a href="#">376608</a> Apple MacOS Big Sur 11.6.6 Not Installed (HT213256)
<a href="#">376612</a> Apple macOS Monterey 12.4 Not Installed (HT213257)
<a href="#">376865</a> IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6565413)
<a href="#">378363</a> IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6565413)
<a href="#">500026</a> Alpine Linux Security Update for apache2
<a href="#">503717</a> Alpine Linux Security Update for apache2
<a href="#">671578</a> EulerOS Security Update for httpd (EulerOS-SA-2022-1569)
<a href="#">671659</a> EulerOS Security Update for httpd (EulerOS-SA-2022-1730)
<a href="#">671739</a> EulerOS Security Update for httpd (EulerOS-SA-2022-1790)
<a href="#">671758</a> EulerOS Security Update for httpd (EulerOS-SA-2022-1807)
<a href="#">671800</a> EulerOS Security Update for httpd (EulerOS-SA-2022-1843)
<a href="#">671812</a> EulerOS Security Update for httpd (EulerOS-SA-2022-1867)
<a href="#">671851</a> EulerOS Security Update for httpd (EulerOS-SA-2022-1893)
<a href="#">690812</a> Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (6601c08d-a46c-11ec-8be6-d4c9ef517024)
<a href="#">710595</a> Gentoo Linux Apache HTTPD Multiple Vulnerabilities (GLSA 202208-20)
<a href="#">730403</a> Apache Hypertext Transfer Protocol (HTTP) Server Out-of-bounds Write Vulnerability
<a href="#">751909</a> SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0928-1)
<a href="#">751912</a> SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0918-1)
<a href="#">751918</a> SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:0929-1)
<a href="#">751936</a> SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:1031-1)
<a href="#">751942</a> OpenSUSE Security Update for apache2 (openSUSE-SU-2022:1031-1)
<a href="#">900758</a> Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (9005)
<a href="#">901955</a> Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (9015-1)
<a href="#">940741</a> AlmaLinux Security Update for httpd:2.4 (ALSA-2022:7647)
<a href="#">940823</a> AlmaLinux Security Update for httpd (ALSA-2022:8067)
<a href="#">960175</a> Rocky Linux Security Update for httpd:2.4 (RLSA-2022:7647)
<a href="#">960481</a> Rocky Linux Security Update for httpd (RLSA-2022:8067)

© [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](#)**