



CVE-2022-24795

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

Summary

CVE	CVE-2022-24795
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-05 16:15:00 UTC
Updated	2023-11-07 03:44:00 UTC
Description	yajl-ruby is a C binding to the YAJL JSON parsing and generation library. The 1.x branch and the 2.x branch of `yajl` contain

Risk And Classification

Problem Types: CWE-190 | CWE-122

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yajl-ruby Project	Yajl-ruby	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 38 Update: yajl-2.1.0-21.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 38 Update: yajl-2.1.0-21.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 37 Update: yajl-2.1.0-21.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Merge pull request #204 from eileencodes/fix-c-warnings · brianmario/yajl-ruby@7168bd7 · GitHub	MISC	github.com
Reallocation bug can trigger heap memory corruption · Advisory · brianmario/yajl-ruby · GitHub	CONFIRM	github.com
[SECURITY] Fedora 37 Update: yajl-2.1.0-21.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] [DLA 3492-1] yajl security update	MLIST	lists.debian.org
[SECURITY] [DLA 3516-1] burp security update	MLIST	lists.debian.org
yajl-ruby/yajl_buf.c at 7168bd79b888900aa94523301126f968a93eb3a6 · brianmario/yajl-ruby · GitHub	MISC	github.com
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

[160247](#) Oracle Enterprise Linux Security Update for yajl (ELSA-2022-7524)

[160291](#) Oracle Enterprise Linux Security Update for yajl (ELSA-2022-8252)

[184196](#) Debian Security Update for ruby-yajl (CVE-2022-24795)

[199554](#) Ubuntu Security Notification for YAJL Vulnerabilities (USN-6233-1)

[200011](#) Ubuntu Security Notification for YAJL Vulnerabilities (USN-6233-2)

[240836](#) Red Hat Update for yajl (RHSA-2022:7524)

[240907](#) Red Hat Update for yajl (RHSA-2022:8252)

[284318](#) Fedora Security Update for yajl (FEDORA-2023-00572178e1)

[284354](#) Fedora Security Update for yajl (FEDORA-2023-852b377773)

[355555](#) Amazon Linux Security Advisory for yajl : ALAS2-2023-2101

[355644](#) Amazon Linux Security Advisory for yajl : ALAS2023-2023-263

[6000034](#) Debian Security Update for burp (DLA 3516-1)

[671722](#) EulerOS Security Update for yajl (EulerOS-SA-2022-1776)

[671834](#) EulerOS Security Update for yajl (EulerOS-SA-2022-1919)

[672332](#) EulerOS Security Update for yajl (EulerOS-SA-2022-2786)

[672357](#) EulerOS Security Update for yajl (EulerOS-SA-2022-2751)

[672420](#) EulerOS Security Update for yajl (EulerOS-SA-2022-2812)

[672433](#) EulerOS Security Update for yajl (EulerOS-SA-2022-2837)

[672449](#) EulerOS Security Update for yajl (EulerOS-SA-2022-2863)

[752161](#) SUSE Enterprise Linux Security Update for libyajl (SUSE-SU-2022:1746-1)

[752560](#) SUSE Enterprise Linux Security Update for libyajl (SUSE-SU-2022:3162-1)

[900813](#) Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-yajl-ruby (9344)

[901350](#) Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-yajl-ruby (9344-1)

[902748](#) Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-yajl-ruby (10552)

[903928](#) Common Base Linux Mariner (CBL-Mariner) Security Update for rubygem-yajl-ruby (10552-1)

[940753](#) AlmaLinux Security Update for yajl (ALSA-2022:7524)

[940835](#) AlmaLinux Security Update for yajl (ALSA-2022:8252)

[960281](#) Rocky Linux Security Update for yajl (RLSA-2022:7524)

[960497](#) Rocky Linux Security Update for yajl (RLSA-2022:8252)

© [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](#)