

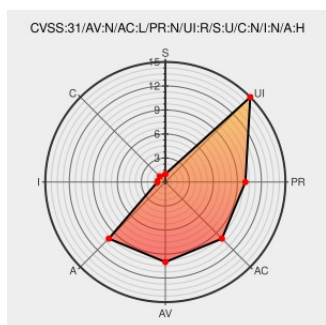


CVE-2023-33460

Published on: Not Yet Published

Last Modified on: 08/05/2023 07:15:00 PM UTC

CVE-2023-33460

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

There's a memory leak in yajl 2.1.0 with use of yajl_tree_parse function. which will cause out-of-memory in server and cause crash.

CVE-2023-33460 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

Attack
Vector

Attack
Complexity

Privileges
Required

User
Interaction

NETWORK

LOW

NONE

REQUIRED

Scope

Confidentiality
Impact

Integrity
Impact

Availability
Impact

UNCHANGED

NONE

NONE

HIGH

CVE References

Description

Tags

Link

[SECURITY] [DLA 3478-1] yajl security update

[lists.debian.org](#)
text/html

[MLIST \[debian-lts-announce\] 20230702](#)
[SECURITY] [DLA 3478-1] yajl security update

[SECURITY] Fedora 38 Update: yajl-2.1.0-21.fc38 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](#)
text/html

[FEDORA FEDORA-2023-00572178e1](#)

[SECURITY] Fedora 37 Update: yajl-2.1.0-21.fc37 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](#)
text/html

[FEDORA FEDORA-2023-852b377773](#)

[SECURITY] [DLA 3492-1] yajl security update

[lists.debian.org](#)
text/html

[MLIST \[debian-lts-announce\] 20230711](#)
[SECURITY] [DLA 3492-1] yajl security update

memory leak in yajl_tree_parse function. · Issue #250 · lloyd/yajl · GitHub

[github.com](#)
text/html

[MISC github.com/lloyd/yajl/issues/250](#)

[SECURITY] Fedora 38 Update: R-jsonlite-1.8.5-2.fc38 - package-announce - Fedora Mailing-Lists

[lists.fedoraproject.org](#)
text/html

[FEDORA FEDORA-2023-0b0bb84049](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

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

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

[284331](#) Fedora Security Update for R (FEDORA-2023-0b0bb84049)

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

[355454](#) Amazon Linux Security Advisory for yajl : ALAS2023-2023-214

[355790](#) Amazon Linux Security Advisory for yajl : ALAS2-2023-2182

[355809](#) Amazon Linux Security Advisory for yajl : ALAS2023-2023-279

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

[6000066](#) Debian Security Update for yajl (DLA 3478-1)

[754272](#) SUSE Enterprise Linux Security Update for libyajl (SUSE-SU-2023:3301-1)

[907023](#) Common Base Linux Mariner (CBL-Mariner) Security Update for yajl (27143-1)

[907078](#) Common Base Linux Mariner (CBL-Mariner) Security Update for yajl (27147-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Yajl Project	Yajl	2.1.0	All	All	All
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:37:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:38:*:*:*:*:*:						
cpe:2.3:a:yajl_project:yajl:2.1.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#)