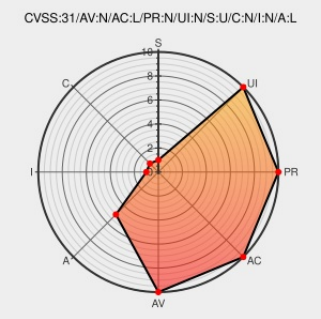
CVE-2021-43838

Published on: Not Yet Published

Last Modified on: 07/21/2023 04:45:00 PM UTC

CVE-2021-43838 - advisory for GHSA-55xv-f85c-248q

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Jsx-slack from Jsx-slack Project contain the following vulnerability:

jsx-slack is a library for building JSON objects for Slack Block Kit surfaces from JSX. In versions prior to 4.5.1 users are vulnerable to a regular expression denial-of-service (ReDoS) attack. If attacker can put a lot of JSX elements into `<blockquote>` tag, an internal regular expression for escaping characters may consume an excessive amount of computing resources. jsx-slack v4.5.1 has patched to a regex for escaping blockquote characters. Users are advised to upgrade as soon as possible.

CVE-2021-43838 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **yhatt** - **jsx-slack** version **< 4.5.1**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Merge pull request from GHSA-55xv-f85c-248q · yhatt/jsx-slack@36e4a10 · GitHub	github.com text/html	MISC github.com/yhatt/jsx-slack/commit/36e4a10405e4c7745333e245fcc5029c02c7065d
Regular Expression Denial of Service (ReDoS) in jsx-slack · Advisory · yhatt/jsx-slack · GitHub	github.com text/html	CONFIRM github.com/yhatt/jsx-slack/security/advisories/GHSA-55xv-f85c-248q

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jsx-slack Project	Jsx-slack	All	All	All	All

cpe:2.3:a:jsx-slack_project:jsx-slack:*:*:*:*:*:node.js:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43838 : jsx-slack is a library for building JSON objects for Slack Block Kit surfaces from JSX. In version… twitter.com/i/web/status/1…	2021-12-17 18:26:06
/r/netcve	CVE-2021-43838	2021-12-17 19:38:06

← Previous ID

Next ID→