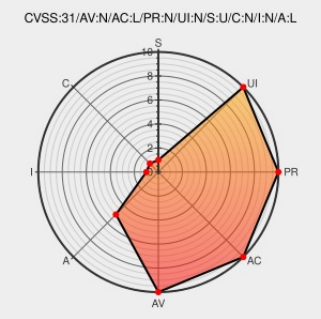
CVE-2021-43843

Published on: Not Yet Published

Last Modified on: 08/09/2022 01:27:00 PM UTC

CVE-2021-43843 - advisory for GHSA-hp68-xhvj-x6j6

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 package for building JSON objects for Slack block kit surfaces from JSX. The maintainers found the patch for CVE-2021-43838 in jsx-slack v4.5.1 is insufficient tfor protection from a Regular Expression Denial of Service (ReDoS) attack. If an attacker can put a lot of JSX elements into `<blockquote>` tag _with including multibyte characters_, an internal regular expression for escaping characters may consume an excessive amount of computing resources. v4.5.1 passes the test against ASCII characters but misses the case of multibyte characters. jsx-slack v4.5.2 has updated regular expressions for escaping blockquote characters to prevent catastrophic backtracking. It is also including an updated test case to confirm rendering multiple tags in `<blockquote>` with multibyte characters.

CVE-2021-43843 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **yhatt** - **jsx-slack** version **< 4.5.2**

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
Release v4.5.2 · yhatt/jsx-slack · GitHub	github.com text/html	MISC github.com/yhatt/jsx-slack/releases/tag/v4.5.2
Insufficient patch for Regular Expression Denial of Service (ReDoS) to jsx-slack v4.5.1 · Advisory · yhatt/jsx-slack · GitHub	github.com text/html	CONFIRM github.com/yhatt/jsx-slack/security/advisories/GHSA-hp68-xhvj-x6j6
Prevent catastrophic backtracking in blockquote escape replacer · yhatt/jsx-slack@46bc883 · GitHub	github.com text/html	MISC github.com/yhatt/jsx-slack/commit/46bc88391d89d5fda4ce689e18ca080bcdd29ecc
Regular Expression Denial of Service (ReDoS) in jsx-slack · Advisory · yhatt/jsx-slack · GitHub	github.com text/html	MISC github.com/yhatt/jsx-slack/security/advisories/GHSA-55xv-f85c-248q

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-2021-43843 : jsx-slack is a package for building JSON objects for Slack block kit surfaces from JSX. The mainta… twitter.com/i/web/status/1…	2021-12-20 21:23:23
/r/netcve	CVE-2021-43843	2021-12-20 22:38:36

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report