



# CVE-2021-43843

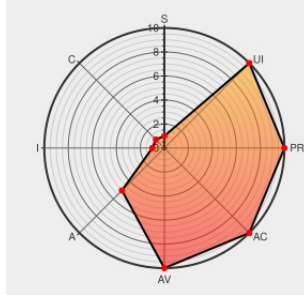
Published on: Not Yet Published

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](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L



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 for 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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
|                        |                   |                     |

NONE

NONE

PARTIAL

CVE References

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

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](mailto: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 | <a href="#">Jsx-slack Project</a> | <a href="#">Jsx-slack</a> | 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2021-12-20 21:23:23 |
| /r/netcve  | <a href="#">CVE-2021-43843</a>                                                                                                                                                                           | 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](https://status.cve.report)