



CVE-2021-23346

Published on: 03/04/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:54 PM UTC

CVE-2021-23346

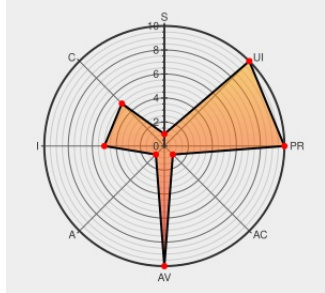
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

IS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/R



Certain versions of [Html-parse-stringify](#) from [Html-parse-stringify Project](#) contain the following vulnerability:

This affects the package html-parse-stringify before 2.0.1; all versions of package html-parse-stringify2. Sending certain input could cause one of the regular expressions that is used for parsing to backtrack, freezing the process.

CVE-2021-23346 has been assigned by report@snyk.io to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

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
html-parse-stringify/parse.js at master · HenrikJoreteg/html-parse-stringify · GitHub	Broken Link Third Party Advisory github.com text/html	MISC github.com/HenrikJoreteg/html-parse-stringify/blob/master/lib/parse.js%23L2

Regular Expression Denial of Service (ReDoS) in org.webjars.npm:html-parse-stringify2 Snyk	Exploit Patch Third Party Advisory snyk.io text/html	 CONFIRM N/A
fixing reported ReDoS · HenrikJoreteg/html-parse-stringify@c7274a4 · GitHub	Patch Third Party Advisory github.com text/html	 CONFIRM N/A
html-parse-stringify2/parse.js at master · rayd/html-parse-stringify2 · GitHub	Broken Link Third Party Advisory github.com text/html	 CONFIRM N/A
Regular Expression Denial of Service (ReDoS) in html-parse-stringify Snyk	Exploit Patch Third Party Advisory snyk.io text/html	 CONFIRM N/A
Regular Expression Denial of Service (ReDoS) in html-parse-stringify2 Snyk	Exploit Patch Third Party Advisory snyk.io text/html	 CONFIRM N/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.

Related QID Numbers

[982913](#) Nodejs (npm) Security Update for html-parse-stringify2 (GHSA-545q-3fg6-48m7)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Html-parse-stringify Project	Html-parse-stringify	All	All	All	All
Application	Html-parse-stringify Project	Html-parse-stringify	All	All	All	All
cpe:2.3:a:html-parse-stringify_project:html-parse-stringify:*:*:*:*:node.js:*:*:						
cpe:2.3:a:html-parse-stringify_project:html-parse-stringify:*:*:*:*:node.js:*:*:						

Discovery Credit

Yeting Li

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](#)