Regular Expression Denial of Service (ReDoS)

Affecting org.webjars.npm:html-parse-stringify2 package, versions **[0,]**

INTRODUCED: 1 MAR 2021 CVE-2021-23346 CWE-400

Share

How to fix?

There is no fixed version for `org.webjars.npm:html-parse-stringify2`.

Overview

org.webjars.npm:html-parse-stringify2 is a This is a fork of html-parse-stringify

Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS). Sending certain input could cause one of the regular expressions that is used for parsing to backtrack, freezing the process.

References

- GitHub Commit
- GitHub PR #2
- html-parse-stringify2 Vulnerable Code
- html-parse-stringify Vulnerable Code

MEDIUM

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High

See more

NVD 5.3 MEDIUM

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-JAVA-ORGWEBJARSNPM-1080633
Published	1 Mar 2021
Disclosed	1 Mar 2021
Credit	Yeting Li

Report a new vulnerability | Found a mistake?

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.