snyk Vulnerability DB

Snyk Vulnerability Database › npm › html-parse-stringify

MEDIUM

Search by package name or CVE

Regular Expression Denial of Service (ReDoS)

Affecting html-parse-stringify package, versions <2.0.1

INTRODUCED: 1 MAR 2021 CVE-2021-23346 CWE-400 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `html-parse-stringify` to version 2.0.1 or higher.

Overview

html-parse-stringify is a https://github.com/henrikjoreteg/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

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 Learn

Learn about Regular Expression Denial of Service (ReDoS) vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-HTMLPARSESTRINGIFY-1079306
Published	1 Mar 2021
Disclosed	1 Mar 2021
Credit	Yeting Li

Report a new vulnerability

Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

Registered in England and Wales. Company number: 09677925

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