HIGH

Search by package name or CVE

Command Injection

Affecting total.js package, versions <3.4.7

INTRODUCED: 29 JAN 2021 CVE-2020-28494 ? CWE-78 ? FIRST ADDED BY SNYK

Share ▾

> ### How to fix?
>
> Upgrade `total.js` to version 3.4.7 or higher.

Overview

total.js is a framework for Node.js platfrom written in pure JavaScript similar to PHP's Laravel or Python's Django or ASP.NET MVC. It can be used as web, desktop, service or IoT application.

Affected versions of this package are vulnerable to Command Injection. The issue occurs in the `image.pipe` and `image.stream` functions. The `type` parameter is used to build the command that is then executed using `child_process.spawn`. The issue occurs because `child_process.spawn` is called with the option `shell` set to `true` and because the `type` parameter is not properly sanitized.

PoC

```
const total = require('total.js'); let image = Image.load(""); let payload = ";touch HACKED;"; image.stream(payload); //
image.pipe(null, payload);
```

References

- GitHub Commit

Snyk CVSS

Exploit Maturity	Proof of concept ?
Attack Complexity	Low ?
Confidentiality	HIGH ?

See more

> NVD   8.6 HIGH

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-JS-TOTALJS-1046672
Published	29 Jan 2021
Disclosed	29 Jan 2021
Credit	Alessio Dellalibera

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

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon   Join the >> community

© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

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