CRITICAL

Search by package name or CVE

Command Injection

Affecting spritesheet-js package, versions *

INTRODUCED: 4 DEC 2020 CVE-2020-7782 ❓ CWE-78 ❓ (FIRST ADDED BY SNYK)

Share ⌄

How to fix?

There is no fixed version for `spritesheet-js` .

Overview

spritesheet-js is a command-line spritesheet (a.k.a. Texture Atlas) generator written in node.js.

Affected versions of this package are vulnerable to Command Injection. It depends on a vulnerable package `platform-command` . The injection point is located in line 32 in lib/generator.js, which is triggered by main entry of the package.

PoC

```
var a =require("spritesheet-js"); a('./', { scale:"& touch JHU #",trim:true});
```

References

- Vulnerable Code

Snyk CVSS

Exploit Maturity	Proof of concept ❓
Attack Complexity	Low ❓
Confidentiality	(HIGH) ❓
Integrity	(HIGH) ❓
Availability	(HIGH) ❓

See more

> NVD   9.8 CRITICAL

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-SPRITESHEETJS-1048333
Published	9 Feb 2021
Disclosed	4 Dec 2020
Credit	JHU System Security Lab

Report a new vulnerability   Found a mistake?

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon

Join the >> community