Arbitrary Command Injection

Affecting ffmpegdotjs package, versions *

INTRODUCED: 23 FEB 2021 CVE-2021-23376 CWE-77 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `ffmpegdotjs` .

Overview

ffmpegdotjs is a FFMPEG module for nodejs

Affected versions of this package are vulnerable to Arbitrary Command Injection. If attacker-controlled user input is given to the `trimvideo` function, it is possible for an attacker to execute arbitrary commands. This is due to use of the `child_process` `exec` function without input sanitization.

PoC (provided by reporter):

```
var ffmpegdotjs = require("ffmpegdotjs"); ffmpegdotjs.trimvideo("package-lock.json",0,30,"n || touch success;
#").then((file)=>{ console.log(file); });
```

(A file called `success` will be created as a result of the execution of `touch success` .)

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-FFMPEGDOTJS-1078542
Published	18 Apr 2021
Disclosed	23 Feb 2021
Credit	OmniTaint

Report a new vulnerability Found a mistake?

Registered in England and Wales. Company number: 09677925

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