MEDIUM

🔍 Search by package name or CVE

Arbitrary Command Injection

Affecting portprocesses package, versions <1.0.5

INTRODUCED: 23 FEB 2021 CVE-2021-23348 ❓ CWE-77 ❓ (FIRST ADDED BY SNYK)

Share ⌄

Snyk CVSS

Exploit Maturity	Proof of concept ❓
Attack Complexity	Low ❓

See more

> NVD `8.8 HIGH`

How to fix?

Upgrade `portprocesses` to version 1.0.5 or higher.

Overview

portprocesses is a This tool letes you list and kill processes on a specified port.

Affected versions of this package are vulnerable to Arbitrary Command Injection. If (attacker-controlled) user input is given to the `killProcess` 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 portprocesses = require('portprocesses'); portprocesses.killProcess('$(touch success)');
```

References

- GitHub Commit
- Vulnerable Code

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-PORTPROCESSES-1078536
Published	31 Mar 2021
Disclosed	23 Feb 2021
Credit	OmniTaint

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

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon | Join the >> community