Arbitrary Command Injection

Affecting kill-by-port package, versions **<0.0.2**

INTRODUCED: 23 FEB 2021 CVE-2021-23363 CWE-77 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `kill-by-port` to version 0.0.2 or higher.

Overview

kill-by-port is a kills process by port

Affected versions of this package are vulnerable to Arbitrary Command Injection. If (attacker-controlled) user input is given to the `killByPort` 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 kill_by_port = require('kill-by-port');


kill_by_port.killByPort('$(touch success)');
```

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

References

- GitHub Commit
- Vulnerable Code

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low

See more

NVD 8.8 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-KILLBYPORT-1078531
Published	30 Mar 2021
Disclosed	23 Feb 2021
Credit	OmniTaint

Report a new vulnerability | Found a mistake?

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

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