Arbitrary Command Injection

Moderate **fishcharlie** published **GHSA-vm67-7vmg-66vm** on Mar 30, 2021

Package

🟥 **portprocesses** (npm)

Affected versions	Patched versions
<= 1.0.4	1.0.5

Description

Impact

An Arbitrary Command Injection vulnerability was reported in `portprocesses` impacting versions <= 1.0.4.

Example (Proof of Concept)

The following example demonstrates the vulnerability and will run `touch success` therefore creating a file named `success`.

```
const portprocesses = require("portprocesses");

portprocesses.killProcess("$(touch success)");
```

Patches

This vulnerability was patched in version 1.0.5.

Workarounds

Users can ensure all arguments being passed to `portprocesses` are sanitized and not malicious.

Credit

Thanks to the following for reporting and assisting with patching this vulnerability.

- OmniTaint
- Snyk

For more information

If you have any questions or comments about this advisory:

- Open an issue in PortProcesses
- Email us at support@rrainn.com

Severity

Moderate

CVE ID

CVE-2021-23348

Weaknesses

No CWEs

Credits

👥 omnitaint