Defend your code against **SpringShell** in two ways: read our **blog post** with what-to-do advice, and use **Checkmarx SCA** to test your applications.

Command Injection Vulnerability In The Proctree NPM Package

`NODE` `NODEJS` `JAVASCRIPT` `NPM` `RCE` `TYPESCRIPT`

Adar Zandberg   Apr 26, 2021

Details   Overview

Summary

The proctree Node.js package is vulnerable to command injection. Exploitation is possible via unsanitized shell metacharacters provided to the fix() function.

Product

All versions of the proctree NPM package.

Impact

This issue may lead to remote code execution on a machine running the proctree.

Steps To Reproduce

```
var PsTree = require('proctree');
PsTree.getProcessTree("; touch HACKED &&")
```

Expected Result:

A file named `HACKED` has been created.

Remediation

No fix is currently available. It is recommended to sanitize every untrusted input used by your applications.

Credit

This issue was discovered and reported by Checkmarx SCA Security Analyst Adar Zandberg.

Resources

1. Vulnerable code index.js#L46