Arbitrary Command Injection

Affecting ps-visitor package, versions *

INTRODUCED: 18 APR 2021 CVE-2021-23374 CWE-77 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `ps-visitor`.

Overview

ps-visitor is a Node.js visit command `ps aux` and `kill`.

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

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

References

- Vulnerable Code

HIGH

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low

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-PSVISITOR-1078544
Published	18 Apr 2021
Disclosed	18 Apr 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.