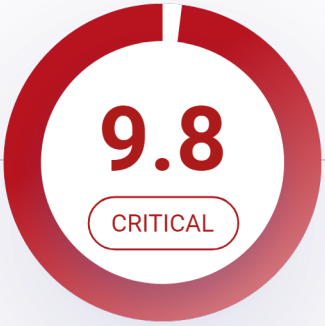
Arbitrary Code Execution

Affecting @pendo324/get-process-by-name package, versions *



Snyk CVSS

Attack Complexity	Low
Confidentiality	HIGH
Integrity	HIGH
Availability	HIGH

See more

NVD 9.8 CRITICAL

INTRODUCED: 7 MAR 2022 CVE-2022-25644
CWE-94 FIRST ADDED BY SNYK

Share

How to fix?

There is no fixed version for `@pendo324/get-process-by-name`.

Overview

@pendo324/get-process-by-name is a Returns a list of processes that match a process name

Affected versions of this package are vulnerable to Arbitrary Code Execution due to improper sanitization of `getProcessByName` function.

PoC

```
const { getProcessByName } = require('@pendo324/get-process-by-name'); getProcessByName("python\" && echo \"1\"> rce.txt # "")
```

References

- 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 Learn

Learn about Arbitrary Code Execution vulnerabilities in an interactive lesson.

Start learning

Snyk ID	**SNYK-JS-PENDO324GETPROCESSBYN/2419094**
Published	**28 Aug 2022**
Disclosed	**7 Mar 2022**
Credit	**Feng Xiao, Zhongfu Su**

Report a new vulnerability

Found a mistake?