New issue

Jump to bottom

Potential command injection vulnerability in npm-dependency-versions #6

Open **xiaofen9** opened this issue on Apr 6 · 0 comments

xiaofen9 commented on Apr 6

Hi,

Thanks for devloping this great npm package! We find a potential command injection vulnerabilty from it. The bug is caused by the fact that package-exported method fail to sanitize `pkgs` parameter and let it flow into a sensitive command execution API.

Here is the proof of concept.

```
const dependencyVersions = require("./index.js")
dependencyVersions({"pkgs":["|touch rce"]})
```

Please consider fix it. thanks!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant