New issue

Jump to bottom

Fix arbitray code execution #6

Merged pillys merged 1 commit into pillys:master from alromh87:master on Oct 6, 2020

Conversation 0 Commits 1 Checks 0 Files changed 2

alromh87 commented on Oct 6, 2020 • edited Contributor

fs-path was vulnerable against arbitrary command injection cause some user supplied inputs were taken and composed into string to be executed without prior validation.
After update Arbitary Code Execution is avoided

Input is sanitized using shell-escape before execution

🦎 Proof of Concept (PoC) *

1. Check there aren't files called HACKED
2. Install package
3. Create poc.js

```
const fspath = require('./lib/');
fspath.copy('./file2','./&whoami>HACKED #', function(err){
        if(err)console.log(err);
        else console.log('ok');
});
```

4. Create input file
   ```
   touch file2
   ```
5. Run poc
   ```
   node poc.js
   ```
6. Recheck files : now HACKED has been created

🔥 Proof of Fix (PoF) *

After fix destination option is correctly treated as a string instead of being executed, file2 is copied to "./&whoami>HACKED #"

👍 User Acceptance Testing (UAT)

Commands can be executed normally

Fix Arbitary Code Execution 88ff5ee

pillys merged commit ef32e31 into pillys:master on Oct 6, 2020

Reviewers
No reviews

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
Successfully merging this pull request may close these issues.
None yet

3 participants