New issue

Jump to bottom

fix: fix prototype pollution vulnerability #13

Merged sahellebusch merged 2 commits into master from fix-proto-poll-vuln on Dec 27, 2020

Conversation 0 Commits 2 Checks 0 Files changed 3

sahellebusch commented on Dec 27, 2020 Owner

From WhiteSource:

The NPM module 'flattenizer' can be abused by Prototype Pollution vulnerability since the function 'unflatten()' did not check for the type of object before assigning value to the property. Due to this flaw an attacker could create a non-existent property or able to manipulate the property which leads to Denial of Service or potentially Remote code execution.

Proof of concept code:

```
var flattenizer = require("flattenizer")
flattenizer.unflatten({'__proto__.polluted': true});
console.log(polluted);
```

sahellebusch added 2 commits 2 years ago

fix: fix prototype pollution vulnerability ··· 26dd347

update docs 6a4ef1c

sahellebusch merged commit 3c6a635 into master on Dec 27, 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

1 participant