

New issue

Jump to bottom

Fix prototype pollution #37

Merged evangelion1204 merged 2 commits into master from fix-prototype-pollution on Dec 10, 2020

Conversation 1 Commits 2 Checks 0 Files changed 8



evangelion1204 commented on Dec 10, 2020 • edited

Owner

Fixed prototype pollution by ignoring __proto__ in sections and keys.

Steps to reproduce
payload.ini

```
[__proto__]
polluted = "polluted"
```

poc.js:

```
var ini = require('multi-ini')

var parsed = ini.read('./payload.toml', { encoding: 'utf8' })
console.log(parsed)
console.log(parsed.__proto__)
console.log({}.__proto__)
console.log(polluted)

> node poc.js
{}
{ polluted: 'polluted' }
{ polluted: 'polluted' }
polluted
```

Michael Iwersen added 2 commits 2 years ago

Fixed prototype pollution

b9ddf8

Bumped version

✓ 4617804

coveralls commented on Dec 10, 2020

coverage 95%

Coverage increased (+0.1%) to 95.111% when pulling 4617804 on fix-prototype-pollution into f494134 on master.



evangelion1204 merged commit 49d6027 into master on Dec 10, 2020
1 check passed

View details

evangelion1204 deleted the fix-prototype-pollution branch 2 years ago

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

2 participants

