New issue

Jump to bottom

Security Fix for Prototype Pollution - huntr.dev #11

Merged eirhor merged 2 commits into Geta:master from 418sec:1-npm-nested-object-assign on Jan 28, 2021

Conversation 1 Commits 2 Checks 0 Files changed 2

huntr-helper commented on Jan 28, 2021 Contributor

@arjunshibu (https://huntr.dev/users/arjunshibu) has fixed a potential Prototype Pollution vulnerability in your repository 🔨. For more information, visit our website (https://huntr.dev/) or click the bounty URL below...

Q | A
Version Affected | *
Bug Fix | YES
Original Pull Request | 418sec#1
Vulnerability README | https://github.com/418sec/huntr/blob/master/bounties/npm/nested-object-assign/1/README.md

User Comments:

📊 Metadata *

`nested-object-assign` is vulnerable to `Prototype Pollution`.

Bounty URL: https://www.huntr.dev/bounties/1-npm-nested-object-assign

⚙️ Description *

Prototype Pollution refers to the ability to inject properties into existing JavaScript language construct prototypes, such as objects.
JavaScript allows all Object attributes to be altered, including their magical attributes such as `__proto__`, `constructor` and `prototype`. An attacker manipulates these attributes to overwrite, or pollute, a JavaScript application object prototype of the base object by injecting other values. Properties on the Object.prototype are then inherited by all the JavaScript objects through the prototype chain.

💻 Technical Description *

Fix implemented by not allowing to modify object prototype.

🦎 Proof of Concept (PoC) *

1. Create the following PoC file:

```
// poc.js
const assign = require('nested-object-assign')

console.log('Before: ' + {}.polluted)
assign({}, JSON.parse('{"__proto__": {"polluted": true}}'))
console.log('After: ' + {}.polluted)
```

2. Execute the following commands in terminal:

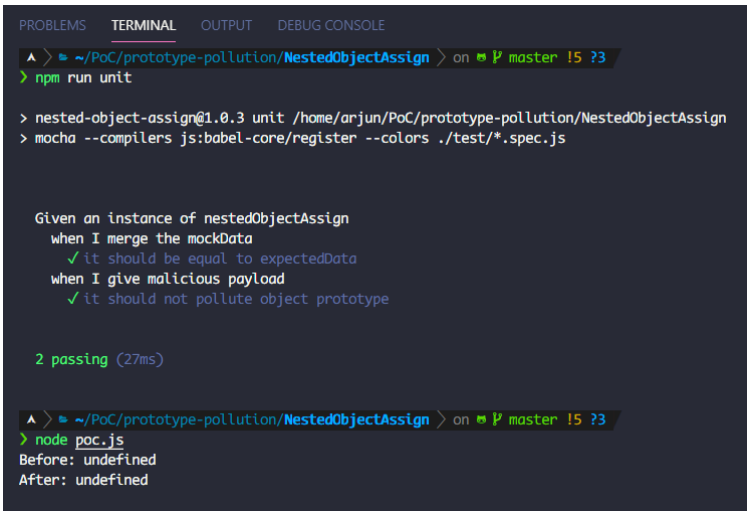
```
npm i nested-object-assign # Install vulnerable package
node poc.js #  Run the PoC
```

3. Check the Output:

```
Before: undefined
After: true
```

🔥 Proof of Fix (PoF) *

I've added unit tests for Prototype Pollution



+1 User Acceptance Testing (UAT)

- I've executed unit tests.
- After fix the functionality is unaffected.

arjunshibu and others added 2 commits 2 years ago

`Security fix for Prototype Pollution` `3a6d2cb`

`Merge pull request #1 from arjunshibu/master` `7df2223`

eirhor self-requested a review 2 years ago

eirhor approved these changes on Jan 28, 2021

View changes

eirhor merged commit `676f6b7` into `Geta:master` on Jan 28, 2021

JamieSlome commented on Feb 20, 2021

@eirhor, if you want more security fixes and patches like this in the future, you can let security researchers know that they can win bounties protecting your repository by copying this small code snippet into your README.md:

```
[![huntr](https://cdn.huntr.dev/huntr_security_badge.svg)](https://huntr.dev)
```

👇 👇 👇

security bounty | up to $750 + CVE

This was referenced on May 9, 2021

Potential Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') (CWE-1321) mesqueeb/copy-anything#10

Closed

[Prototype Pollution] https://github.com/mesqueeb/copy-anything/issues/10 mesqueeb/copy-anything#11

Open

debricked bot mentioned this pull request on Jul 9, 2021

Bulk vulnerability fix - Lockfile fix WeDoSoftware/webAppBackend#253

Open

Reviewers

eirhor ✓

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

4 participants