43

# Http request splitting

Share:

TIMELINE

arkadiyt submitted a report to Node.js.

Sep 14th (4 years ago)

Hi,

I came upon the following tweet today: https://twitter.com/YShahinzadeh/status/1039396394195451904

which details a http request splitting vulnerability in NodeJS. You can confirm it with the following repro script:

**Code** 331 Bytes Wrap lines Copy Download

```
const http = require('http')

const server = http.createServer((req, res) => {
  console.log(req.url);
  res.end();
});

server.listen(8000, function() {
  http.get('http://127.0.0.1:8000/?param=x\u{0120}HTTP/1.1\u{010D}\u{010A}Host:{\u012
  });
});
```

The vulnerability seems to be fixed in v10.0.0 but still present in v8.12.0. I also couldn't find a CVE for it or any information in the NodeJS changelog about it, so I'm not sure if the NodeJS community is aware of the issue.

Should this bug get a CVE assigned / have the fix backported to Carbon?

## Impact

Http request splitting

mylesborins Node.js staff posted a comment. Sep 16th (4 years ago)

Hey Arkady,

Thanks for submitting. I'll bring this to the team and get back to you this week.

mylesborins Node.js staff added weakness "HTTP Response Splitting". Sep 16th (4 years ago)

mylesborins Node.js staff updated the severity to Medium (5.3). Sep 16th (4 years ago)

mylesborins Node.js staff changed the status to ○ **Triaged**. Sep 16th (4 years ago)

I can confirm that 8.x and 6.x are vulnerable to this attack, where 10.x is not.

The Internet Bug Bounty has decided that this report is not eligible for a bounty. Sep 16th (4 years ago)

Unfortunately this report does not qualify for a bounty as "only critical vulnerabilities that demonstrate complete compromise of the system's integrity or confidentiality are eligible for a bounty - typically Arbitrary Code Execution or equivalent impact. While we encourage you to submit all potential issues, lower severity issues are not in scope at this time."

If you disagree with this assessment please let me know and we can revisit.

mylesborins Node.js staff posted a comment. Sep 25th (4 years ago)

We have a fix that is being reviewed. We are also picking a date for a security release. Will keep you updated

arkadiyt posted a comment. Oct 23rd (4 years ago)

Any updates on the release date for this?

mcollina Node.js staff posted a comment. Oct 24th (4 years ago)

We have a security release being planned for mid-november. Unfortunately there was a lot of overlap between already scheduled releases.

mylesborins Node.js staff posted a comment. Nov 1st (4 years ago)

I'll update you if anything changes. Thank you so much for your patience.

arkadiyt posted a comment. Nov 1st (4 years ago)

Great thanks for the update!

rvagg posted a comment. Nov 24th (4 years ago)

Hey @arkadiyt, a fix for this is going out on the 27th as per https://nodejs.org/en/blog/vulnerability/november-2018-security-releases/ and I'm trying to put together an attribution for it. I'm thinking of something along the lines of "Originally discovered by Twitter user @YShahinzadeh and reported to Node.js by `<your name here>`". If you'd like to have your name in that, would you mind telling me how you'd like to be listed, and optionally an organisation with which you are affiliated. Cheers.

arkadiyt posted a comment. Nov 24th (4 years ago)

Sure, can I be listed as Arkadiy Tetelman with the organization Lob?

Thanks very much,

mylesborins Node.js staff closed the report and changed the status to ○ **Resolved**. Nov 27th (4 years ago)

The latest version of 6.x and 8.x are out with this fix. Thanks for reporting. You can see more details on our blog

https://nodejs.org/en/blog/vulnerability/november-2018-security-releases/#http-request-splitting-cve-2018-12116

octetcloud requested to disclose this report. Jan 14th (3 years ago)

arkadiyt agreed to disclose this report. Jan 14th (3 years ago)

This report has been disclosed. Jan 14th (3 years ago)