

0 Open redirect in fastify-static via mishandled user's input when attempt to redirect

Share:     

TIMELINE



drstrnegth submitted a report to Fastify.

Sep 28th (about 1 year ago)

Summary:

When fastify-static is mounted at root and the register option `redirect: true`, the following 2 lines cause open redirect bug: <https://github.com/fastify/fastify-static/blob/master/index.js#L156-L157>. A remote attackers can redirect users to arbitrary web sites via a double forward slash: `://`, for example if attacker wants to redirect to google.com: `http://<domain_name>//google.com/%2e%2e`.

This bug is similar to [CVE-2015-1164](https://expressjs.com/en/advanced/security-updates.html) in ExpressJS, they published on their page about the security bugs here (you can Ctrl+F and search for [CVE-2015-1164](https://expressjs.com/en/advanced/security-updates.html)): <https://expressjs.com/en/advanced/security-updates.html>

Steps To Reproduce:

1. Download my PoC [here](#)
2. `bash run.sh`
3. Use Firefox to navigate to `http://localhost:3000//google.com/%2e%2e`. You will see that you are redirected to <https://www.google.com/>

Request:

Code 102 Bytes [Wrap lines](#) [Copy](#) [Download](#)

```
1 GET //google.com/%2e%2e HTTP/1.1
2 Host: localhost:3000
3 Accept-Encoding: gzip, deflate
4 Connection: close
```

Response:

Code 133 Bytes [Wrap lines](#) [Copy](#) [Download](#)

```
1 HTTP/1.1 301 Moved Permanently
2 Location: //google.com/%2e%2e/
3 content-length: 0
4 Date: Wed, 29 Sep 2021 03:34:22 GMT
5 Connection: close
```

I tested and it only works in Firefox but not in Chrome, Edge, Opera, Safari 🤔, it is because different browsers handle the response differently.

Impact

The most straight-forward impact is phishing.

However, open redirect is a gadget that enables attackers to be able to exploit further, for example:

- Bypassing SSRF protection
- Token stealing in OAuth

1 attachment:

[F1464894: fastify-static-poc.zip](#)



mcollina Fastify staff changed the status to Triaged.

Oct 1st (about 1 year ago)

Thanks for reporting. This is exactly like the expres bug. We will issue a security release as quickly as possible.

For completenss, Here is the fix express did in 2015: <https://github.com/expressjs/serve-static/issues/26>



mcollina Fastify staff posted a comment.

Oct 1st (about 1 year ago)

I propose <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N&version=3.1> as CVSS score. Do you agree?

How could we credit this finding to you?

Unfortunately we are unable to offer bounties at the minute.



eomm joined this report as a participant.

Oct 1st (about 1 year ago)



drstrnegth posted a comment.

Oct 1st (about 1 year ago)

Hi, thank you for replying.

I am happy with CVSS 3.7. To credit my finding, could you list the bug founder in the CVE as "drstrnegth"?

I didn't find vulnerability in Fastify for bounty so it is okay for me not receiving bounty.

In the future, can I write a blog about this CVE?
































drstrnegth posted a comment.

Oct 1st (about 1 year ago)

To be more precise about the fix by Express, this is their commit that fix the bug: <https://github.com/expressjs/serve-static/commit/0399e399935bab99530d6926094b4451438c2d50>

mcollina Fastify staff posted a comment

Oct 1st (about 1 year ago)

 Ah very sorry, it is my first time reporting on Hackerone so I got a mistake. You can download the PoC in the attachment, its name is "fastify-static-poc.zip"	
  posted a comment.  How can we credit this vulnerability to you?	Oct 4th (about 1 year ago)
 posted a comment. Can you issue a CVE and list me as the bug founder?	Oct 4th (about 1 year ago)
  posted a comment. Yes, that's what the question was for.	Oct 4th (about 1 year ago)
  posted a comment. Can you issue a CVE and list me as the bug founder?	Oct 4th (about 1 year ago)
yes! How can I attribute it to you?	
 posted a comment. I think we can issue a CVE on https://cveform.mitre.org/ , and then we can attach reference to this report through URL. What do you think?	Oct 4th (about 1 year ago)
  posted a comment. I will request it from HackerOne right now. I would just need some text to attribute the finding to you. If you do not want this to be attributed to you let me know, I've asked 3 times already :D.	Oct 4th (about 1 year ago)
  posted a comment. I didn't see it: <div>I am happy with CVSS 3.7. To credit my finding, could you list the bug founder in the CVE as "drstrnegth"?</div> yes, that's totally ok.	Oct 4th (about 1 year ago)
 posted a comment. It seems I miscommunicated with you somewhere in the process. Yes, please refer me as "drstrnegth". Thank you	Oct 4th (about 1 year ago)
  updated CVE reference to CVE-2021-22963 .	Oct 5th (about 1 year ago)
  updated the severity from Low to <u>Low</u> (3.7).	Oct 5th (about 1 year ago)
  closed the report and changed the status to Resolved . Fixed in fastify-static v4.2.4	Oct 5th (about 1 year ago)
  requested to disclose this report.	Oct 5th (about 1 year ago)
 posted a comment. Hi, I just checked the new version and found the fix is insufficient. <ul style="list-style-type: none"> 1: the author changed from using the package url to new URL() but without try catch, I can DOS the server 2: I can still redirect user to arbitrary website Should I open another report or continue here?	Oct 6th (about 1 year ago)
  posted a comment. Thanks for the check! Please open a fresh report. Please include all script to reproduce.	Oct 6th (about 1 year ago)
 posted a comment. Should I open another report or continue here? To speed up the process, could you share more info here as a preview to replicate? I was unable to trigger a DOS and the redirect Thanks	Oct 7th (about 1 year ago)
 posted a comment. Weird, I reproduce on my linux server seems to happily accept <code>curl --path-as-is "http://localhost:3000/^.."</code> without any crash. Nevertheless, I change the payload to <code>curl --path-as-is "http://localhost:3000/://.."</code> and still got DOS. For your convenient, I attach my screen record. 1 attachment: F1474467: fastify-dos-open-redirect.mp4	Oct 7th (about 1 year ago)
 posted a comment. Oh I see why, my NodeJS version in localhost is v15.10.0, which will throw error when it meet character "^" in domain name, that's why in my report I used <code>curl --path-as-is "http://localhost:3000/://.."</code> ; However, my NodeJS version on my linux server is 14.17.6 and it does not throw. I attached below an image below for you to compare.	Updated Oct 7th (about 1 year ago)



drstrnegth posted a comment.

Deleted (please ignore this comment)

Updated Oct 7th (about 1 year ago)



drstrnegth agreed to disclose this report.

Oct 11th (about 1 year ago)



This report has been disclosed.

Oct 11th (about 1 year ago)