22 **[Uppy] Internal Server side request forgery (bypass of #786956)**

Share:

TIMELINE

mahmoud0x00 submitted a report to Node.js third-party modules. Jun 4th (3 ye

I would like to report `Internal Server-side request forgery` in Uppy
It allows the attacker to easily extract information from internal servers

Module

module name: Uppy
version:1.15.0
npm page: `https://www.npmjs.com/package/uppy`

Module Description

Uppy is a sleek, modular JavaScript file uploader that integrates seamlessly with any application. It's fast, easy to use and lets you worry about more important problems than building a file uploader.

Module Stats

[1] weekly downloads: 37,599

Vulnerability

Server-Side Request Forgery (SSRF)
Vulnerability Description

When I checked your fix on #786956, I noticed that you fixed this issue by doing a check on the host 's IP address against a blacklist before passing it to the server fetch (You can check that here, But you forgot to stop redirection to these IP addresses, therefore attacker can create a host or file and redirect all requests which being received to a specific internal host, this will bypass your check, in the first phase, System will check if this host is allowed or no, if it is allowed, Server will pass request. But it won't be able to verify which host is being redirected to.

Steps To Reproduce:

- feel free to set up a custom Uppy version on your server and try these steps on

1. Go to https://uppy.io/
2. Choose download file via a link
3. Pass this link to the system `https://tinyurl.com/gqdv39p` (it redirects to `http://169.254.169.254/metadata/v1/`)
4. Upload fetched file
5. Download that file
6. Open that file and you should see a copy of DigitalOcean 's metadata host response [redacted]

Supporting Material/References:

[redacted]

Wrap up

> Select Y or N for the following statements:

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

Impact

Unauthorized access to sensitive info on internal hosts/services.

h01_analyst_jake HackerOne triage changed the status to **Needs more info**. Jun 5th (3 ye

Hi @mahmoud0x00,

Thanks for your report. I'm having difficulties reproducing the described behavior. Specifically, passing the TinyURL link results in the following error message:

Code 65 Bytes Wrap lines Copy Dow

```
1 Companion failed to fetch this URL, please make sure it’s correct
```

Could you double-check on your side?

Best,
@lugtag

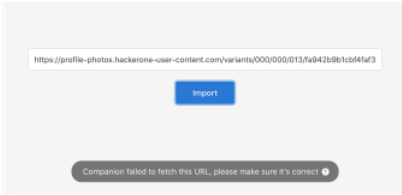
mahmoud0x00 changed the status to **New**. Jun 5th (3 ye

a strange behavior occurred, On Firefox it fetches the file and while Uploading it, the server responds with `Failed to Upload` while on chrome it responds with thi response `Companion failed to fetch this URL, please make sure it’s correct` similar to what you got. It was working yesterday (Look into my video)

mahmoud0x00 posted a comment. Updated Jun 5th (3 ye

Hey,

seems it is a problem in their setup, seems that someone noticed that I fetched sensitive file yesterday and disabled it. Try to fetch any file using URL and it will thr the same error. (this on chrome)



So to reproduce it, feel free to set up the latest version of it on your local machine and follow the same steps to reproduce it. or you can invite the maintainer of the module and let him triage it.

Thanks

1 attachment:
F856169: Screen_Shot_2020-06-05_at_1.51.18_PM.png

mahmoud0x00 posted a comment. Jun 5th (3 ye

Hey @lugtag,

it came back to work, Please triage it as soon as possible.

Thanks

h1_analyst_jake HackerOne triage changed the status to **Triaged**. Jun 8th (3 ye

Hello @mahmoud0x00,

Thank you for your submission! We were able to validate your report, and have submitted it to the appropriate remediation team for review. They will let us know t final ruling on this report, and when/if a fix will be implemented. Please note that the status and severity are subject to change.

Regards,
@lugtag

h1_analyst_jake HackerOne triage updated the severity from Critical (10.0) to Critical (9.3). Jun 8th (3 ye

arturi joined this report as a participant. Jun 15th (3 ye

arturi posted a comment. Jun 15th (3 ye

Thanks for reporting! Could you please invite ife@transloadit.com?

mahmoud0x00 posted a comment. Jun 15th (3 ye

@arturi Thanks for replying, Could you please create a CVE for this one? after fixing it for sure, I don't have the ability to invite other users, I guess @lugtag can hel this

danielruf Node.js third-party modules staff posted a comment. Jun 18th (3 ye

I have invited the person as requested. So it is already fixed and we can disclose this report and request a CVE?

ifedapoolarewaju joined this report as a participant. Jun 18th (3 ye

ifedapoolarewaju posted a comment. Jun 18th (3 ye

@danielruf It is not fixed yet. There's a PR to fix it here https://github.com/transloadit/uppy/pull/2322 but it hasn't been released yet, so we can hold-off on the C for now. Also thank you for the invitation

ifedapoolarewaju posted a comment. Jun 18th (3 ye

For clarity, the fix from #786956 did address redirects. However, this current issue only occurs when the original URL being requested has a different protocol (e.g from the protocol it redirects to (e.g https). For example the URL https://tinyurl.com/gqdv39p (with protocol https) redirects to http://169.254.169.254/metadat (with protocol http) and so the issue could be reproduced. The PR description explains this.

danielruf Node.js third-party modules staff posted a comment. Jun 18th (3 ye

Thanks for the clarification @ifedapoolarewaju.

Regarding the CVE, we can request one only after the disclosure of the report which is done after the issue is fixed.

mahmoud0x00 posted a comment. Jun 20th (2 ye

@ifedapoolarewaju @arturi @danielruf

I have just noticed that you mentioned this issue in Changelog yesterday, also I have already checked this issue on your demo version and it seems fixed, Good Jol

ifedapoolarewaju posted a comment. Updated Jun 22nd (2 ye

Yes, this is correct. The issue has been fixed (on versions 1.13.2, and 2.0.0-alpha.5) and released via npm. Thank you again for reporting the issue 🙏

mahmoud0x00 posted a comment. Jun 22nd (2 ye

You are welcome @ifedapoolarewaju 🙏 @danielruf time for disclosure and CVE request?

mahmoud0x00 posted a comment. Jun 22nd (2 ye

Hi @mahmoud0x00, I have redacted (converted to internal-only) the screenshot and the video from the initial report. Is this correct or do we have to redact more

mahmoud0x00 posted a comment. Jun 28th (2 ye

@danielruf Looks good 👍

danielruf Node.js third-party modules staff closed the report and changed the status to **Resolved**. Jun 28th (2 ye

danielruf Node.js third-party modules staff requested to disclose this report. Jun 28th (2 ye

mahmoud0x00 agreed to disclose this report. Jun 28th (2 ye

This report has been disclosed. Jun 28th (2 ye