Exposure of Sensitive Information to an Unauthorized Actor in transloadit/uppy

0

Valid Reported on Feb 3rd 2022

Description

First thanks to my friend Haxatron for this awsome report
I review the `@uppy/companion` code from the source to the sink, and I figure out a significant issue that makes any SSRF protection Effectless.
I put myself as a Developer and started to read the companion document, and then I saw Debug option explanation:

```
debug(optional) - A boolean flag to tell Companion whether to log useful debug information while running.
```

So we have three options for Debug: 1. `true` and 2. `false` and 3. `default value` that the default value set to true according to this line of code.
Many developers usually don't set optional values, and Also others want to use the debug information.
According to the `downloadURL` method, the default value of `blockLocalIPs` is oposite of the `req.companion.options` (that has a `true` value in default and debug mode) .
So we have a `false` value for `blockLocalIPs` often, Let's see where the `blockLocalIPs` will be used :
The `blockLocalIPs` passed Into getRedirectEvaluator and getProtectedHttpAgent methods
The Mentioned methods are used for validating the URLs and IPs for SSRF issues, and as their second input is `false` most of the time, Then no SSRF protection will be done.
I also ran for myself companion server with this example code `uppy-with-companion` , manipulated the inputs to local IP addresses, and made an SSRF attack. (in both dubug=true and false cases)

Impact

A user with URL upload access could enumerate internal companion server networks, send local webservers files to the destination server, and finally download them If each of these files had a guessable and regular name.

Fix suggestion

I think Uppy could use another option (a new one) to let users choose whether uploading from the internal network is legal or not, the default value should be `false` .

CVE
CVE-2022-0528
(Published)

Vulnerability Type
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity
Medium (6.5)

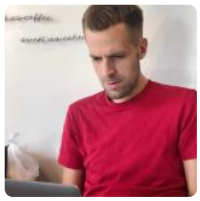
Visibility
Public

Status
Fixed

Found by

amammad
@amammad
pro

Fixed by



Mikael Finstad
@mifi
maintainer

This report was seen 508 times.

We are processing your report and will contact the **transloadit/uppy** team within 24 hours.
10 months ago

amammad modified the report 10 months ago

amammad modified the report 10 months ago

We have contacted a member of the **transloadit/uppy** team and are waiting to hear back

10 months ago

We have sent a follow up to the **transloadit/uppy** team. We will try again in 7 days. 10 months ago

Mikael Finstad validated this vulnerability 10 months ago

amammad has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

We have sent a fix follow up to the **transloadit/uppy** team. We will try again in 7 days. 10 months ago

We have sent a second fix follow up to the **transloadit/uppy** team. We will try again in 10 days. 9 months ago

We have sent a third and final fix follow up to the **transloadit/uppy** team. This report is now considered stale. 9 months ago

Mikael Finstad marked this as fixed in **3.3.1** with commit **267c34** 9 months ago

Mikael Finstad has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation