Server Side Request Forgery via location header in jgraph/drawio

0

Valid Reported on May 15th 2022

Description

It is possible to bypass current SSRF checks using a redirection via the location header.

Proof of Concept

1.) Mock a redirect endpoint using https://beeceptor.com/
2.) Add `Location: http://localhost:1122` as a response header and set the status code to 301
3.) Listen on port 1122
4.) Access the following resource: `/proxy?url=http://<id>.free.beeceptor.com` (`http` is important here)
5.) The request will be made to localhost:1122

From my understanding the code implements its own redirection handling by reading the location header and doing a new request. But this happens after `setInstanceFollowRedirects` is set to true. By setting it to true the connection will follow redirects automatically before any checks.

Impact

This vulnerability is capable of doing requests controlled by an attacker and leaking sensitive information to an attacker.

References

- Similar issue

CVE
CVE-2022-1767
(Published)

Vulnerability Type
CWE-918: Server-Side Request Forgery (SSRF)

Severity
High (7.5)

Registry
Other

Affected Version
18.0.4

Visibility
Public

Status
Fixed

Found by

myxl
@myyxl
pro

This report was seen 736 times.

We are processing your report and will contact the **jgraph/drawio** team within 24 hours.
6 months ago

myxl modified the report 6 months ago

myxl modified the report 6 months ago

myxl modified the report 6 months ago

myxl modified the report 6 months ago

David Benson 6 months ago

Hi, do you have a video showing the PoC attack working?

myxl 6 months ago Researcher

Hi, thanks for responding, I can record one if that's preferable, I'll get back to you soon!

David Benson 6 months ago

Thanks. It's just for a critical we need to be absolutely sure it's scored correctly. A lot of users will have to update their source.

myxl 6 months ago Researcher

Here is the link to the video: https://streamable.com/5uhbks
If the report gets verified I would like to delete the video again, for privacy reasons, if that's okay.
The top terminal shows the output of the docker container, the left one a shell session inside the docker container and the right one a curl command to invoke to SSRF.

David Benson 6 months ago

I've accepted this as critical, I don't think it's critical on reflection. I don't care about the bounty, but is it possible to re-score this @admin @jamieslome ?

Jamie Slome 6 months ago Admin

@davidjgraph - you are still able to re-score this using the `Edit` button at the top right of the report next to the severity.

Let me know if you are having any issues with this 👍

David Benson modified the Severity from Critical (9.3) to High (8.6) 6 months ago

David Benson modified the Severity from High (8.6) to High (7.5) 6 months ago

myxl 6 months ago Researcher

Seems good!

David Benson 6 months ago

@myyxl , sorry, I posted that on the wrong issue. We are testing the setInstanceFollowRedirects

behaviour to double check. If correct, a 7.5 is about right for such a SSRF.

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

David Benson validated this vulnerability 6 months ago

myxl has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

David Benson 6 months ago

18.0.7 release contains the fix,
https://github.com/jgraph/drawio/commit/c63f3a04450f30798df47f9badbc74eb8a69fbdf

myxl 6 months ago Researcher

Looks good to me!

David Benson marked this as fixed in **18.0.7** with commit **c63f3a** 6 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

.

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

company

about

team