SSRF in /service endpoint in jgraph/drawio

0

✓ Valid Reported on May 20th 2022

Description

The problem came from this line of code
I ran `docker-drawio` with following command :
`docker run -it --rm --name="draw" -e EXPORT_URL=http://somesite.com -p 8080:8080 -p 8443:8443 jgraph/drawio`
if the drawio `EXPORT_URL` is set to an address without any `/` after the primary Hostname like `http://somesite.com` (not like `http://somesite.com/something` or `http://somesite.com/`), then an attacker can send a request to `127.0.0.1:4431` with a payload like `http://draio-instance/service/0/@127.0.0.1:4431`

Proof of Concept

run `docker run -it --rm --name="draw" -e EXPORT_URL=http://google.com -p 8080:8080 -p 8443:8443 jgraph/drawio` and then `docker ps` and get the drawio hash name (called HN)
run `docker exec -it HN /bin/bash`
run `apt update && apt install netcat && netcat -l 4430`
go to `http://draio-instance:8080/service/0/@127.0.0.1:4431` you can see the http log on netcat had been recorded
it is a Full SSRF If you need another POC I can give you an HTTP logger script that returns some things to the attacker
11
Also, I don't know what exactly is `JSESSIONID` cookie? but I can receive its content in a My public IP after redirect too!

Impact

The impact is achieved to all internal http webservers' contents if they host a file with a short and enumerable name! Or get cloud metadata, port scanning, and some special cases achieve RCE too!
However, it is an Open-redirect too.
about the CVSS: `Attack Complexity` is high because this vulnerability depends on some

special configuration for EXPORT_URL. `Availability` is none `Confidentiality` and `Availability` can be high as it is a full SSRF.
I think 7.4 is a good score if you don't please tell me to change it, please.

CVE
CVE-2022-1815
(Published)

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

Severity
Medium (5.3)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

amammad
@amammad
pro

This report was seen 803 times.

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

amammad modified the report 6 months ago

amammad 6 months ago

Researcher

Hey David, can you ping somethings to me about this report?

Chat with us

We have contacted a member of the **jgraph/drawio** team and are waiting to hear back
6 months ago

David Benson 6 months ago

Hey. We're thinking about this one (please also consider it's the weekend and we're not working). I'd say the integrity affect is low, following the guidance on https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator, since it's dependent on a number of server setup factor, the integrity effect is certainly not high in every case, and would be none for certain setups.

amammad modified the report 6 months ago

amammad modified the report 6 months ago

amammad 6 months ago Researcher

I made a mistake. The attack complexity is not high because, as you say, because of the server setup factor, the integrity should be none, and also attack complexity about how we can exploit the founded vulnerability. Here the exploit is simple. even not need any server for DNS rebinds or redirection URLs.
So do you agree with `5.3` ?

David Benson validated this vulnerability 6 months ago

Yes, I think medium overall is right for this issue. We'll investigate it today.

amammad has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

amammad 6 months ago Researcher

I'm glad to see we're on the same page!

David Benson marked this as fixed in 18.1.2 with commit c287be 6 months

Chat with us

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ×

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us