huntr

SSRF in editor's proxy via IPv6 link-local address in jgraph/drawio

0

✓ Valid Reported on May 13th 2022

Description

The proxy server does not check for link-local IPv6 addresses
In
https://github.com/jgraph/drawio/blob/dev/src/main/java/com/mxgraph/online/ProxyServlet.java#L255L257, it checks for local IP addresses. It is missing the link-local IPv6 address check - https://docs.oracle.com/javase/7/docs/api/java/net/InetAddress.html#isLinkLocalAddress()

Proof of Concept

1: Setup Wireshark 2: In your local copy of the DrawIO webapp open:
http://localhost:8080/draw/proxy?url=%68%74%74%70%3a%2f%2f%5b%66%65%38%30%3a%3a%31%5d
3: The server, takes a while as it attempts to connect to [fe80::1], the default gateway (seen from Wireshark logs) - denoting that fe80:: link-local IPv6 addresses are not being filtered.

Impact

SSRF to internal link-local IPv6 addresses

CVE
CVE-2022-1722
(Published)

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

Severity
High (7.5)

Registry
Other

Affected Version
Online Editor

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

This report was seen 799 times.

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

haxatron modified the report 6 months ago

haxatron 6 months ago Researcher

Hi, I think this may be a false positive due to how Java INetAddress works (though I am not too sure). INetAddress will cache the 1st resolution so the 2nd resolution will not work.

I think I have another possible bypass to this if you give me the permission to test it.

Side note: Would it be possible to set up a "Safe Harbor" policy (like programs on Bugcrowd) so that security researchers will be at ease when testing the website.

David Benson 6 months ago Maintainer

Hey. Yes, we need safe habour details, as well as a full in-scope section on this site. The admins are working on creating that, in the meantime I think we'll put it in the security.md on the repos.

If you mean test on app.diagrams.net, you're welcome to, but note that we don't actually use this proxy code due to security concerns :). The node code we use is Cloudflare Workers specific we wanted to publish code that people could use freely across a number of p

There is a Java deployment at https://drawdotio.appspot.com, that's probably the better place to test.

haxatron 6 months ago Researcher

Alright, thanks. Is the particular proxy code linked in scope?

David Benson 6 months ago Maintainer

Yeah, since people can deploy it on their own projects. We've a bit of discussion around this, but if you find a valid hole we'll pay. If there is a rebinding attack it's certain the same value as the original find.

haxatron 6 months ago Researcher

Alright, thanks! I'll investigate!

haxatron 6 months ago Researcher

Hi do you have an internal IP I can hit on appspot.com to prove the SSRF?

haxatron 6 months ago Researcher

The 2nd bypass I had in my mind was IPv6 address, the code only check IPv4 and not IPv6 so addresses such as [::] which points to localhost and the IP4-IPv6 embedded mapped addresses. As I am away from the computer right now, I cannot spin a Java instance to test this. I will investigate further when I get home.

haxatron 6 months ago Researcher

Correction: the code can check for ::, but I don't think it can check for ::ffff:a9fe:a9fe, which is ipv6 representation for 169.254.169.254 and the private ipv6 ranges such as fe80:: and so on

David Benson 6 months ago Maintainer

https://cloud.google.com/compute/docs/internal-dns are the docs relating to GCP internal DNS. The internal IP is 169.254.169.254 for metadata calls. I'm not aware that GCP e address for that, but then, that's the whole of this test :).

haxatron 6 months ago Researcher

Thanks for that, the appspot.com doesnt seem vulnerable because google metadata requires the special Metadata header, though the code is still vulnerable to link-local IPv6 addresses and IPv4-IPv6 embedded mapping addresses. I'll probably spin a local instance and test everything by tonight and consolidate the details.

David Benson 6 months ago Maintainer

Cool. I would add that I think the integrity and availability scores shouldn't be high if the attack applies to specific systems. We'd need a PoC that demonstrates an effect on these two factors.

haxatron 6 months ago Researcher

Yep, I initially was basing it on ability to attack Google metadata service, though I was wondering if you consider the scenario where the code runs on other metadata services (though I am not sure if the code is configured to run on other cloud services).

Will probably get all of this sorted by tonight.

David Benson 6 months ago Maintainer

The idea is the project would run on any standard servlet engine. If you found a hole on a reasonable Tomcat setup using this proxy that'd be valid.

There's a seperate project for GAE deployments, https://github.com/jgraph/drawio-app-engine. It's not technically in-scope atm, but I can't see a case where we wouldn't pay out under this project for a hole there.

We're looking to pay bounties actively for anything reasonable, rather than trying to avoid doing so. We want maximum eyeballs on this stuff.

haxatron modified the report 6 months ago

haxatron 6 months ago Researcher

I've investigated this further via my local webapp and found that
[X] DNS Rebinding does not work
[X] IPv4-IPv6 embedded mapping does not work

[V] Link-local IPv6 addresses (fe80::) works

haxatron 6 months ago Researcher

I have updated the report accordingly

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

David Benson validated this vulnerability 6 months ago

haxatron has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

haxatron 6 months ago Researcher

Can confirm 18.0.5 fixes the problem

David Benson 6 months ago Maintainer

Cool, thanks for your detailed analysis and feedback.

David Benson marked this as fixed in **18.0.5** with commit **cf5c78** 6 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us