huntr

SSRF in embed2 servlet via redirects in jgraph/drawio

1

✓ Valid Reported on May 17th 2022

Description

Embed2Servlet uses url.OpenConnection() in https://github.com/jgraph/drawio/blob/7a68ebe22a64fe722704e9c4527791209fee2034/src/main/java/com/mxgraph/online/EmbedServlet2.java#L400 which follows redirects by default. However, the redirections are not being checked, hence it is possible to perform SSRF this way.

Proof of Concept

1: Start a redirector (redirect.php) and an ngrok server

```
<?php

header("Location: http://[fe80::1]");
```

```
ngrok http 80
```

2: Hit your ngrok server to redirect and see response go to fe80::1

```
https://[DIAGRAMS-SERVER]/embed2.js?fetch=http://[NGROK-ID].ngrok.io/redire
```

Recommended Fix

setInstanceFollowRedirects to false in url.openConnection() in Embed2Servlet

Impact

SSRF

Chat with us

CVE
CVE-2022-1784

(Published)

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

Severity
High (7.5)

Registry
Other

Affected Version
<= 18.0.7

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

This report was seen 788 times.

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

David Benson 6 months ago Maintainer

Thanks for the report. Please provide exact environment and reproduction steps.

haxatron 6 months ago Researcher

I am unable to get embed2servlet working locally but I can confirm that the c
which runs 18.0.7 does follow redirects. I tested with fe80::1 and I can reproduc
time which I observed in the link-local bypass.

David Benson 6 months ago Maintainer

Are you saying fe80::1 is an internal IP address?

haxatron 6 months ago Researcher

What I mean is that fe80::1 is included in the link-local filter in https://github.com/jgraph/drawio/blob/7a68ebe22a64fe722704e9c4527791209fee2034/src/main/java/com/mxgraph/online/Utils.java#L511, if it was being properly filtered, the request will not take so long. But it did.

I did that as I cannot interact with embed2.js on my Docker instance locally and the only way to prove that it is not being filtered is via the main site.

haxatron 6 months ago Researcher

*embed2.js returns an error on the local Docker instance.

haxatron modified the report 6 months ago

haxatron modified the report 6 months ago

haxatron 6 months ago Researcher

Updated report with more details. Embed2Servlet uses the url.openConnection in https://github.com/jgraph/drawio/blob/7a68ebe22a64fe722704e9c4527791209fee2034/src/main/java/com/mxgraph/online/EmbedServlet2.java#L400. The initial URL passed is checked against, but since url.openConnection follows redirects by default, the filter is not used for the redirection URLs. Hence, it is possible to perform SSRF this way.

David Benson 6 months ago Maintainer

Redirects are not followed by default, which version of the code are you looking at?

haxatron 6 months ago

They are, https://drawdotio.appspot.com/embed2.js?fetch=https://httpbin.org/redirect-to%3Furl=https://example.com will return URL encoded form of example.com to%3Furl=https://example.com will return URL encoded form of example.com

David Benson 6 months ago Maintainer

ah, so setInstanceFollowRedirects is true by default? Ouch.

haxatron 6 months ago Researcher

Yes, and the redirections are not being checked.

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

David Benson marked this as fixed in 18.0.8 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

2022 © 418sec

huntr

home

part of 418sec

company

Chat with us

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

about

team

Chat with us