Local file inclusion in jgraph/drawio

2

Valid Reported on May 14th 2022

Description

https://app.diagrams.net/embed2.js?&fetch= is used to fetch data and i tried to perform ssrf by extracting google cloud metadata but was unable to do but i am still able to fetch server files like /etc/passwd.

Proof of Concept

```
1. Visit https://app.diagrams.net/embed2.js?&fetch=
2. Enter file:///etc/passwd in fetch parameter and see the content of /etc/
3. Decode the url data and you can see the contents of /etc/passwd where th
```

Impact

An attacker could read local files on the web server that they would normally not have access to, such as the application source code or configuration files containing sensitive information on how the website is configured.

Occurrences

EmbedServlet2.java L387-L431

CVE
CVE-2022-1723
(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

0x2374
@0x2374
unranked

This report was seen 798 times.

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

0x2374 6 months ago Researcher

POC Video Link : https://drive.google.com/file/d/1e0OSr0AI9Jc7yeO1VW8GK2cWIjGn8tWd/view

David Benson 6 months ago

Thanks for the report. Why have you marked the effort on availability as high? That means you know of an attack that would bring the system down, what is that attack please?

0x2374 6 months ago Researcher

Hello David,

LFI can lead to Remote code execution in certain cases if combined with file
vulnerability.

Currently I am only able to achieve Local File Inclusion where I am able to read Web Server Files as explained in the original report.
I didn't tried to check if i am able to achieve RCE will update if i am able to perform until then you can change the CVSS score to **AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N**

I have added an link to blog where it explained impact of LFI : https://brightsec.com/blog/local-file-inclusion-lfi/

Please let me know if you have questions.
Thankyou

David Benson modified the Severity from Critical (9.1) to High (7.5) 6 months ago

0x2374 6 months ago Researcher

Hi David please verify report with the new CVSS score as RCE seems to be not achievable.

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

David Benson validated this vulnerability 6 months ago

Hi, yes, I think this score is appropriate for the LFI alone.

0x2374 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

0x2374 6 months ago Researcher

Hello David just confirming another SSRF report has the same impact as mine please have a look.
https://huntr.dev/bounties/cad3902f-3afb-4ed2-abd0-9f96a248de11/

Thanks

David Benson 6 months ago

Hi, yes, the CVE score on that one is too high.

0x2374 6 months ago Researcher

No it is Critical (9.3)

David Benson 6 months ago

The availability score is not none, but it should have been none.

0x2374 6 months ago Researcher

yes

0x2374 6 months ago Researcher

will you change the cvss to match with that report?

David Benson 6 months ago

There is no mechanism in huntr to do that.

0x2374 6 months ago Researcher

ok no problem

David Benson 6 months ago

cf5c78aa0f3127fb10053db55b39f3017a0654ae changed to high severity

David Benson marked this as fixed in 18.0.6 with commit 7a68eb 6 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

EmbedServlet2.java#L387-L431 has been validated ✓

Sign in to join this conversation