huntr

No rate limit via proxy url parameter in jgraph/drawio

0

✓ Valid Reported on Aug 29th 2022

Description

Hi Drawio Team ,
Your proxy server has no limit of requests which an attacker can use it as PORT SCANNER.
https://app.diagrams.net/proxy?url={IP:PORT}&base64=1

Proof of Concept

Image from my OWASP ZAP : https://ibb.co/h87hz3N

Impact

Malicious use.
Load on memory (DOS).
Effect the availability.

References

- https://cwe.mitre.org/data/definitions/284.html

CVE
CVE-2022-3065
(Published)

Vulnerability Type
CWE-284: Improper Access Control

Severity
Medium (5.3)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

maakthon
@maakthon
amateur

This report was seen 741 times.

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

maakthon modified the report 3 months ago

David Benson 3 months ago Maintainer

Thanks for the report. You're reporting two things here:

DoS. Rate limiting / dealing with DoS is an infrastructure level issue. You will not be able to DoS app.diagrams.net with this attack, we have infrastructure in place to deal with this.

If someone deployed the java ProxyServlet that would be up to them to deal with the issue.

No port filtering. This is valid, but your current rating of critical is incorrect for this one item.

maakthon 3 months ago Researcher

Hi Mr David ,

Thank you for response , So we can count one bug which is [No port filtering]
I will edit it now !

maakthon modified the report 3 months ago

maakthon 3 months ago Researcher

Is it okay now or we have to edit something else Mr David ?

David Benson 3 months ago Maintainer

You've set the effect on integrity and availability as high for the port scanning report, could you explain in detail why those two levels?

maakthon 3 months ago Researcher

Sure,
Imagine someone disclose your proxy in public , So a lot of people will use it as port scanner and put your domain at risk like (someone can use it to scan private or military systems) So if a lot of people used it that will effect the availability.

About the integrity, Sorry I forget to remove it while editing the report.

maakthon modified the report 3 months ago

David Benson modified the Severity from High (7.4) to Medium (5.3) 3 months ago

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

David Benson validated this vulnerability 3 months ago

maakthon has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

maakthon 3 months ago Researcher

Thank you Mr.David.

Chat with us

David Benson marked this as fixed in 20.2.8 with commit 59887e 3 months ago

The fix bounty has been dropped ×

This vulnerability will not receive a CVE ×

maakthon 2 months ago Researcher

@admin
How can I get the bounty ?

maakthon 2 months ago Researcher

Status = Processing , What is that mean?

Pavlos a month ago Admin

Just checking in @maakhton did you get your bounty?

maakthon a month ago Researcher

Yes, Thank you for your interest.

Sign in to join this conversation

2022 © 418sec

huntr

home

part of 418sec

company

Chat with us