

## 0

The application reflects an input from the url without sanitizing it. With a csp bypass from apis.google.com its possible to execute javascript code.

[https://app.diagrams.net/?ui=min&p=tickets#\\_TICKETS%7B%22ticketsConfig%22%3A%7B%7D%7D](https://app.diagrams.net/?ui=min&p=tickets#_TICKETS%7B%22ticketsConfig%22%3A%7B%7D%7D)



## XSS, Phishing

(Published)

## CWE-79: Cross-site Scripting (XSS) - DOM

Medium (6.5)

Chat with us

Registry

Other

Affected Version

20.5.0

Visibility

Public

Status

Fixed

Found by



Joao Vitor Maia

@joaovitormaia

legend ▼



This report was seen 840 times.

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

22 days ago

**David Benson** validated this vulnerability 22 days ago

Another good catch

**Joao Vitor Maia** 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 **20.5.2** with commit **d37894** 20 days ago

The fix bounty has been dropped ✗

This vulnerability has been assigned a CVE ✓

**tickets.js#L83** has been validated ✓

Chat with us

David Benson published this vulnerability 20 days ago



Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us