

# XSS via Mathematical Typesetting in jgraph/drawio

1



Reported on Sep 13th 2022



## Requirements

**Feature:** Extras > Mathematical Typesetting enabled.

**User interaction:** Access vulnerable page || diagram and wheel click on a link.



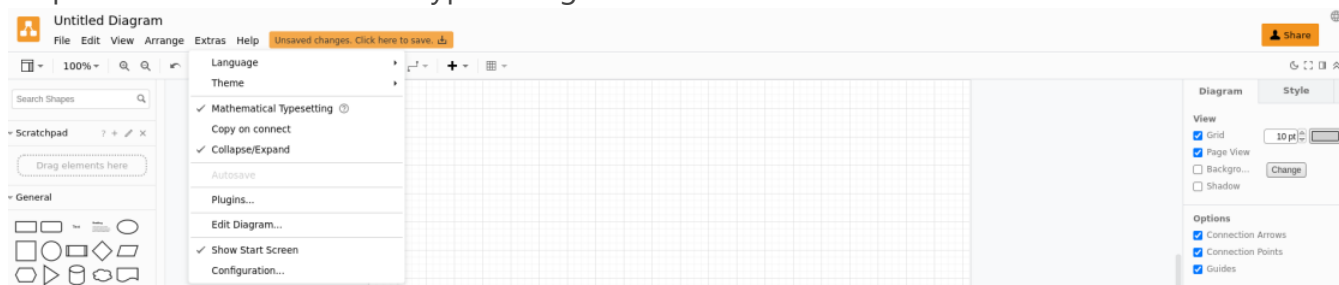
## Description

The [Mathematical Typesetting](#) feature allows to use inline content such as [AsciiMath](#) or [LaTeX](#). Using it allows you to create [a](#) tag via `\href` macro. By default, it allows you to use dangerous wrappers like `javascript:` which permits on click XSS. (wheel click in draw.io context)



## Proof of Concept

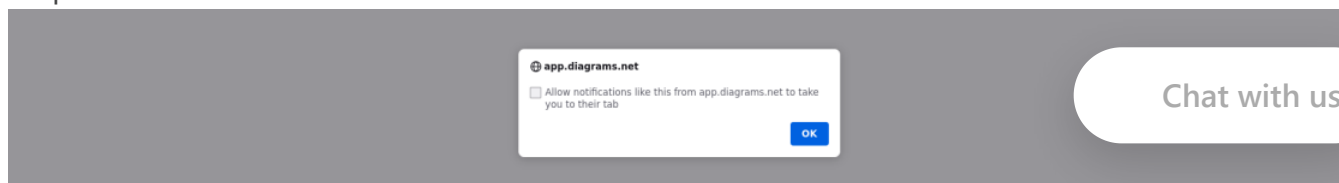
Step 1: Enable Mathematical Typesetting.



Step 2: Copy | Past `$$\href{javascript:alert()}{CLICK}$$` in the diagram.



Step 3: Wheel click on the link.



Check Requierements section if it's not working.

## 🔧 Fix suggestion

Use [ui/safe](#) extension which prevents several security risks such as `javascript` wrapper in the `href` attribute.

## Impact

An attacker might use it, for example, to extract information from the user's diagram.

CVE

CVE-2022-3223

(Published)

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Severity

Medium (4.3)

Registry

Npm

Affected Version

20.2.8

Visibility

Public

Status

Fixed

Found by



Mizu

@kevin-mizu

pro ▼

This report was seen 3,030 times.

Chat with us

We are processing your report and will contact the [jgraph/drawio](#) team within 24 hours.

2 months ago

2 months ago

David Benson 2 months ago

Maintainer

What domain are you testing this on? What is the CSP in the response headers for that domain?

Mizu 2 months ago

Researcher

I tested it on [app.diagrams.net](https://app.diagrams.net) and [viewer.diagrams.net](https://viewer.diagrams.net). But, I got really weird issues testing it, it must be due to CSP, you are right

Mizu 2 months ago

Researcher

Do you want me to take time trying to exploit it with CSP bypass or this is enough for you?

Mizu 2 months ago

Researcher

As an example: [PoC](#)

Mizu modified the report 2 months ago

Mizu modified the report 2 months ago

David Benson 2 months ago

Maintainer

Nothing happens on this PoC for me. What is the CSP in the reponse header for you?

We have contacted a member of the [jgraph/drawio](#) team and are waiting to hear back  
2 months ago

Mizu 2 months ago

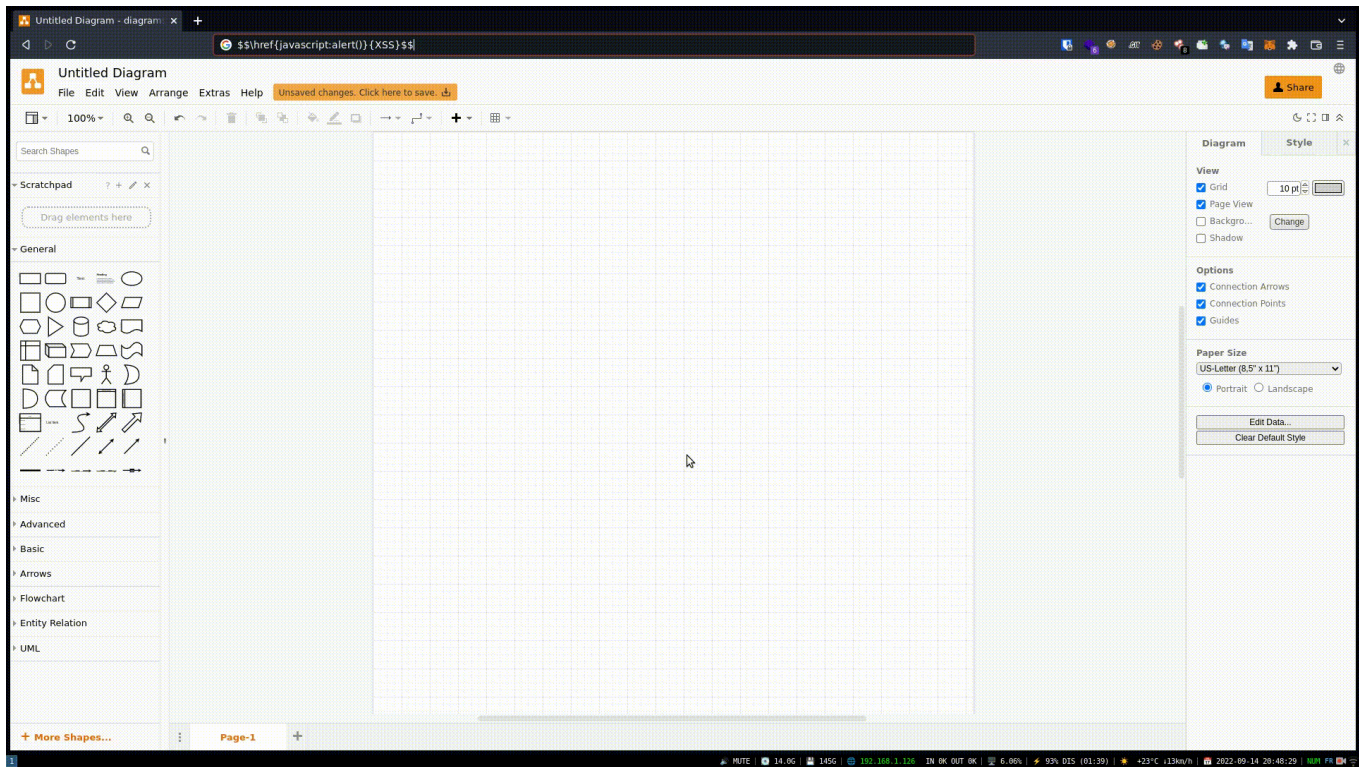
Researcher

CSP on [viewer.diagrams.net](https://viewer.diagrams.net):

```
connect-src *; img-src * data: blob;; media-src * data;; font-src * data:; style-src * data:; script-src * data:;
```

Chat with us

Video:



PS: it must be a wheel click or it won't work.

Diagram: [Link](#)

The PoC doesn't work on [app.diagrams.net](#), I probably did something weird while testing...

David Benson validated this vulnerability 2 months ago

Mizu 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 20.3.1 with commit **ea012b** 2 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Chat with us



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