

XSS at https://viewer.diagrams.net/ in jgraph/drawio

1



Reported on Sep 5th 2022

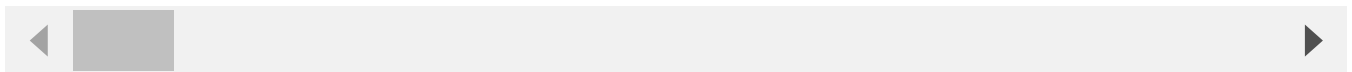
Description

The application uses a parameter to specify a url on the refresh and the back button, assigning it to location.href without sanitizing

Proof of Concept

Go to:

`https://viewer.diagrams.net/index.html?tags=%7B%7D&highlight=0000ff&&layers:`



Click on the refresh or the back icon on toolbar

Impact

XSS, phishing

Occurrences

JS EditorUi.js L2819

JS EditorUi.js L2555

CVE

CVE-2022-3138

(Published)

Vulnerability Type

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

Severity

Medium (4.3)

Chat with us

Registry

Other

Affected Version

20.2.8

Visibility

Public

Status

Fixed

Found by



Joao Vitor Maia

@joaovitormaia

legend ▼



This report was seen 1,860 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

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 **b5dfeb** 3 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

EditorUi.js#L2555 has been validated ✓

EditorUi.js#L2819 has been validated ✓

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