Stored XSS on drawio in jgraph/drawio

6

Valid Reported on May 15th 2022

Sumary

Draw io has a feature to put links on a text, due to a bad sanitization it allows to put javascript:// scheme on a anchor tag which allows to execute javascript code

Steps to reproduce

Create a text box and set word size to 50
Click with the rigth button and "Edit link"
Put asdf://test.com
Click with the rigth button again and "Edit data"
On the "link" attribute put javascript:javascript://%0aalert(document.domain)
Export the page as URL
Click on the link

Impact

It also affects confluence as its available as an app on the marketplace, POC video: https://youtu.be/RHevZOx1nhc

References

- Video POC for Confluence
- Diagram with XSS

CVE
CVE-2022-1730
(Published)

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

Severity
Medium (6.3)

Registry
Other

Affected Version
<= 18.0.3

Visibility
Public

Status
Fixed

Found by

Joao Vitor Maia
@joaovitormaia
legend

This report was seen 1,031 times.

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

David Benson validated this vulnerability 6 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 gave praise 6 months ago

Thank you for correctly scoring the fix initially. There's many attempts to simply score everything as critical, we do remember when researchers score professionally.

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

David Benson marked this as fixed in **18.0.4** with commit **4deece** 6 months

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ×

Joao Vitor Maia 6 months ago

Researcher

Appreciate that!

Sign in to join this conversation