September 9, 2022

GHSL-2022-030: Cross-Site Scripting (XSS) in Jodit Editor 3 - CVE-2022-23461

GitHub Security Lab

Coordinated Disclosure Timeline

- 2022/05/12: Report sent to security@xdsoft.net
- 2022/05/12: Maintainer replies vulnerability is no longer reproducible, they created custom sanitization functions
- 2022/05/13: Bypass sent to maintainer
- 2022/06/12: Asked for status update to maintainer
- 2022/08/10: Deadline expired
- 2022/09/06: CVE-2022-23461 assigned

Summary

Jodit Editor 3 is vulnerable to XSS attacks when pasting specially constructed input.

Product

Jodit Editor 3

Tested Version

3.16.5

Details

Issue: XSS in jodit editor (`GHSL-2022-030`)

This query highlights several locations, all of which I believe to be exploitable. I *believe* this is the location triggered by the PoC.

PoC:

1. Open https://cdn.sekurak.pl/copy-paste/playground.html in your browser, enter the text below in the HTML Input box:

```
<html>
  <body>
  <meta name=Generator content="Microsoft Word 15">
  <img src="" onerror="alert(123)" />
  </body>
</html>
```

1. Click `Copy as HTML`.
2. Go to https://xdsoft.net/jodit/
3. Paste the text you copied in [3].
4. Click `Keep`.
5. JavaScript: `alert(123)` is executed.

Impact

This issue may lead to XSS in any webpage that uses the editor. Users who copy-paste content from a page controlled by an attacker may be vulnerable.

CVE

- CVE-2022-23461

Credit

This issue was discovered by CodeQL team members @kaeluka (Stephan Brandauer) and @erik-krogh (Erik Krogh Kristensen), using a CodeQL query originally contributed by community member @bananabr (Daniel Santos).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include a reference to `GHSL-2022-030` in any communication regarding this issue.

- Atom
- Electron
- GitHub Desktop

Support

- Docs
- Community Forum
- Professional Services
- Status
- Contact GitHub

Company

- About
- Blog
- Careers
- Press
- Shop