August 18, 2022

# GHSL-2022-029: XSS in Toast UI Grid - CVE-2022-23458

GitHub Security Lab

## Coordinated Disclosure Timeline

- 2022/05/12: Opened an issue asking for a security contact
- 2022/05/16: Asked for a security contact oss@nhn.com (Undelivered)
- 2022/06/12: Asked for a security contact dohyung.ahn@nhn.com
- 2022/06/21: daeyeon.kim@nhn.com contacts the Security Lab regarding the opened issue
- 2022/06/21: Report sent to daeyeon.kim@nhn.com
- 2022/07/14: The vulnerability is fixed.
- 2022/08/12: `CVE-2022-23458` assigned.

## Summary

The `nhn/tui.grid` component is vulnerable to XSS attacks when pasting specially crafted content into editable cells.

## Product

Toast UI Grid

## Tested Version

4.21.1

## Details

### Issue: XSS pasting HTML in editable cell (`GHSL-2022-029`)

There is a vulnerability when specially crafted html content is pasted in an editable cell.

**PoC:**

1. Open https://cdn.sekurak.pl/copy-paste/playground.html
2. Paste `<img src="" onerror="alert(123)" />` into the HTML Input box and click `Copy as HTML`
3. Go to https://ui.toast.com/tui-grid
4. Double click an input cell (eg. one in the “Artist” column), and paste the HTML you copied in [2].
5. Exit the cell by clicking any other cell.
6. JavaScript: `alert(123)` is executed.

#### Impact

This issue may lead to XSS.

## Resources

- Fix commit.

## CVE

- CVE-2022-23458

## 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-2022-029` in any communication regarding this issue.

## Product

- Features
- Security
- Enterprise
- Customer stories
- Pricing
- Resources

## Platform

- Developer API
- Partners
- Atom
- Electron
- GitHub Desktop

## Support

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

## Company

- About
- Blog
- Careers
- Press
- Shop

- 
- f
- ▶
- in
-

-
- Terms
- Privacy
- Cookie settings