

Overall Rating - Critical



This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of a DOM-based XSS in `src/muya/lib/contentState/pasteCtrl.js` in MarkText 0.17.1 and before on Windows, Linux and macOS allows arbitrary JavaScript code to run in the context of MarkText main window.

Technical Details

This vulnerability can be exploited if a user copies text from a malicious webpage and paste it into MarkText.

This vulnerability is rated as a **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify [VRM](#) with any questions or concerns you may have.

References

- [CVE-2023-2318](#)
- <https://github.com/marktext/marktext/issues/3618>
- <https://starlabs.sg/advisories/23/23-2318/>