Cross-site scripting vulnerability in TinyMCE

High lnewson published GHSA-27gm-ghr9-4v95 on Jan 28, 2020

Package

tinymce (npm composer nuget)

Affected versions

>=5.0.0 <5.1.4, <4.9.7

Patched versions

4.9.7, 5.1.4

Description

Impact

A cross-site scripting (XSS) vulnerability was discovered in: the core parser, `paste` and `visualchars` plugins. The vulnerability allowed arbitrary JavaScript execution when inserting a specially crafted piece of content into the editor via the clipboard or APIs. This impacts all users who are using TinyMCE 4.9.6 or lower and TinyMCE 5.1.3 or lower.

Patches

This vulnerability has been patched in TinyMCE 4.9.7 and 5.1.4 by improved parser logic and HTML sanitization.

Workarounds

The workarounds available are:

- disable the impacted plugins
- manually sanitize the content using the `BeforeSetContent` event (see below)
- upgrade to either TinyMCE 4.9.7 or TinyMCE 5.1.4

Example: Manually sanitize content

```
editor.on('BeforeSetContent', function(e) {
  var sanitizedContent = ...; // Manually sanitize content here
  e.content = sanitizedContent;
});
```

Acknowledgements

Tiny Technologies would like to thank Michał Bentkowski for discovering this vulnerability.

References

https://www.tiny.cloud/docs/release-notes/release-notes514/#securityfixes

For more information

If you have any questions or comments about this advisory:

- Open an issue in the TinyMCE repo
- Email us at infosec@tiny.cloud

Severity

High

CVE ID

CVE-2020-17480

Weaknesses

No CWEs