

1Panel-dev / MaxKB Public

<> Code Issues 60 Pull requests Actions Security and quality 19 Insights

# Commit 7230daa

shaohuzhang1 authored on Dec 29, 2025 · 1/2 · Verified

fix: Markdown editor xss attack (#4578)

1 parent [159997c](#) commit 7230daa

1 file changed +46 -1

↑ Top ⚙️

Filter files...

- ui/src
  - chat.ts

Search within code ⚙️

```

ui/src/chat.ts
@@ -12,7 +12,8 @@ import i18n from '@/locales'
12 12 import Components from '@/components'
13 13 import directives from '@/directives'
14 14
15 - import { config } from 'md-editor-v3'
15 + import { getDefaultWhiteList } from 'xss'
16 + import { config, XSSPlugin } from 'md-editor-v3'
16 17 import screenfull from 'screenfull'
17 18
18 19 import katex from 'katex'
@@ -43,6 +44,50 @@ config({

```

```
43 44     instance: mermaid,
44 45     },
45 46   },
47 +   markdownItPlugins(plugins) {
48 +     return [
49 +       ...plugins,
50 +       {
51 +         type: 'xss',
52 +         plugin: XSSPlugin,
53 +         options: {
54 +           xss() {
55 +             return {
56 +               whitelist: Object.assign({}, getDefaultWhiteList(), {
57 +                 video: ['src', 'controls', 'width', 'height', 'preload',
'playsinline'],
58 +                 source: ['src', 'type'],
59 +                 input: ['class', 'disabled', 'type', 'checked'],
60 +                 iframe: [
61 +                   'class',
62 +                   'width',
63 +                   'height',
64 +                   'src',
65 +                   'title',
66 +                   'border',
67 +                   'frameborder',
68 +                   'framespacing',
69 +                   'allow',
70 +                   'allowfullscreen',
71 +                 ],
72 +               }),
73 +             onTagAttr: (tag: string, name: any, value: any) => {
74 +               if (tag === 'video') {
75 +                 // 禁止自动播放
76 +                 if (name === 'autoplay') return ''
77 +
78 +                 // 限制 preload
79 +                 if (name === 'preload' && ![ 'none',
'metadata' ].includes(value)) {
80 +                   return 'preload="metadata"'
81 +                 }

```

```
82 +         }
83 +         return undefined
84 +     },
85 +     }
86 +     },
87 +     },
88 +     },
89 + ]
90 + },

46 91 })
47 92 const app = createApp(App)
48 93 app.use(createPinia())
```

Comments 0

Placeholder for comments, showing a profile picture and a text input area.