Clipboard-based DOM-XSS

Low koddsson published GHSA-gpfj-4j6g-c4w9 on Aug 12, 2021

Package

@github/paste-markdown (npm)

Affected versions	Patched versions
< 0.3.3	0.3.4

Description

Impact

A self Cross-Site Scripting vulnerability exists in the @github/paste-markdown library. If the clipboard data contains the string `<table>`, a **div** is dynamically created, and the clipboard content is copied into its **innerHTML** property without any sanitization, resulting in improper execution of JavaScript in the browser of the victim (the user who pasted the code). Users directed to copy text from a malicious website and paste it into pages that utilize this library are affected.

The following @github/paste-markdown code snippet is triggered when the user pastes something and the browser's clipboard data contains an entry whose content-type is **text/HTML**.

```
function generateText(transfer: DataTransfer): string | undefined {
  if (Array.from(transfer.types).indexOf('text/html') === -1) return

  let html = transfer.getData('text/html')
  if (!/<table/i.test(html)) return

  html = html.replace(/<meta.*?>/, '')

  const el = document.createElement('div')
  el.innerHTML = html
  const tables = el.querySelectorAll('table')

  for (const table of tables) {
    if (table.closest('[data-paste-markdown-skip]')) {
      table.replaceWith(new Text(table.textContent || ''))
    }
    const formattedTable = tableMarkdown(table)
    table.replaceWith(new Text(formattedTable))
  }

  return el.innerHTML
}
```

Patches

A security patch was released in version 0.3.4.

Workarounds

A Content Security Policy that prevents `unsafe-inline` helps reduce the likelihood of this vulnerability being exploited in modern browsers.

Severity

Low

CVE ID

CVE-2021-37700

Weaknesses

CWE-79

Credits

bananabr