RUSTSEC-2021-0063

History · Edit

XSS in `comrak`

Reported	May 4, 2021
Issued	May 4, 2021 (last modified: November 6, 2021)
Package	comrak (crates.io)
Type	Vulnerability
Categories	format-injection
Keywords	#xss
Aliases	CVE-2021-38186
Details	https://github.com/kivikakk/comrak/releases/tag/0.10.1
Patched	`>=0.10.1`

Description

comrak operates by default in a "safe" mode of operation where unsafe content, such as arbitrary raw HTML or URLs with non-standard schemes, are not permitted in the output. This is per the reference GFM implementation, cmark-gfm .

Ampersands were not being correctly escaped in link targets, making it possible to fashion unsafe URLs using schemes like `data:` or `javascript:` by entering them as HTML entities, e.g. `&#x64&#x61&#x74&#x61&#x3a`. The intended behaviour, demonstrated upstream, is that these should be escaped and therefore harmless, but this behaviour was broken in comrak.