RUSTSEC-2021-0074

History · Edit

Incorrect handling of embedded SVG and MathML leads to mutation XSS

Reported	July 8, 2021
Issued	July 8, 2021 (last modified: November 6, 2021)
Package	ammonia (crates.io)
Type	Vulnerability
Categories	format-injection
Keywords	#html #xss
Aliases	CVE-2021-38193
Details	https://github.com/rust-ammonia/ammonia/pull/142

Patched	`>=3.1.0`
	`>=2.1.3, <3.0.0`

Description

Affected versions of this crate did not account for namespace-related parsing differences between HTML, SVG, and MathML. Even if the `svg` and `math` elements are not allowed, the underlying HTML parser still treats them differently. Running cleanup without accounting for these differing namespaces resulted in an "impossible" DOM, which appeared "safe" when examining the DOM tree, but when serialized and deserialized, could be exploited to inject abitrary markup.

To exploit this, the application using this library must allow a tag that is parsed as raw text in HTML. These elements are:

- title
- textarea
- xmp
- iframe
- noembed
- noframes
- plaintext
- noscript
- style
- script

Applications that do not explicitly allow any of these tags should not be affected, since none are allowed by default.