jqlang / jq Public

Code Issues 358 Pull requests 87 Discussions Actions Wiki

Commit 2f09060

itchyny and wader committed yesterday · 29 / 30

```
Fix out-of-bounds read in jv_parse_sized()

This fixes CVE-2026-39979.

Co-authored-by: Mattias Wadman <mattias.wadman@gmail.com>
```

master

1 parent 0c7d133 commit 2f09060

1 file changed +2 -1 lines changed

Top

Filter files…

src

jv_parse.c

1 file changed +2 -1 lines changed

Search within code

src/jv_parse.c

```
@@ -893,8 +893,9 @@ jv jv_parse_sized_custom_flags(const char* string, int
length, int flags) {
893  893
894  894      if (!jv_is_valid(value) && jv_invalid_has_msg(jv_copy(value))) {
895  895        jv msg = jv_invalid_get_msg(value);
896       -    value = jv_invalid_with_msg(jv_string_fmt("%s (while parsing '%s')",
     896  +    value = jv_invalid_with_msg(jv_string_fmt("%s (while parsing '%.*s')",
897  897                                                  jv_string_value(msg),
     898  +                                               length,
898  899                                                  string));
899  900        jv_free(msg);
```

```
900   901       }
```

Comments 0

Please sign in to comment.