jqlang / jq Public

Code Issues 358 Pull requests 87 Discussions Actions Wiki

Commit fdf8ef0

tlsbollei authored and itchyny committed 5 days ago · 29 / 30

Add runtime type checks to f_string_indexes

This fixes CVE-2026-39956.

master

1 parent e47e56d commit fdf8ef0

2 files changed +17 -0 lines changed

Top

Filter files…

- src
  - builtin.c
- tests
  - jq.test

2 files changed +17 -0 lines changed

Search within code

src/builtin.c

```
@@ -1306,6 +1306,14 @@ static jv f_string_explode(jq_state *jq, jv a) {
1306 1306  }
1307 1307
1308 1308  static jv f_string_indexes(jq_state *jq, jv a, jv b) {
     1309 +  if (jv_get_kind(a) != JV_KIND_STRING) {
     1310 +    jv_free(b);
     1311 +    return type_error(a, "cannot be searched, as it is not a string");
     1312 +  }
     1313 +  if (jv_get_kind(b) != JV_KIND_STRING) {
     1314 +    jv_free(a);
```

```
        1315 +      return type_error(b, "is not a string");
        1316 +    }
1309    1317       return jv_string_indexes(a, b);
1310    1318     }
1311    1319
```

tests/jq.test

```
         @@ -1549,6 +1549,15 @@ split("")
1549    1549     "xabababababx"
1550    1550     [1,7,[1,3,5,7]]
1551    1551
        1552 + # _strindices is used by indices/1 but is callable
        1553 + try _strindices("abc") catch .
        1554 + 123
        1555 + "number (123) cannot be searched, as it is not a string"
        1556 +
        1557 + try _strindices(123) catch .
        1558 + "abc"
        1559 + "number (123) is not a string"
        1560 +
1552    1561     # trim
1553    1562     # \u000b is vertical tab (\v not supported by json)
1554    1563     map(trim), map(ltrim), map(rtrim)
```

Comments 0

Please sign in to comment.