jqlang / jq Public

Code Issues 358 Pull requests 87 Discussions Actions Wiki

Commit 6374ae0

itchyny committed yesterday · 29 / 30

Fix NUL truncation in the JSON parser

This fixes CVE-2026-33948.

master

1 parent fdf8ef0 commit 6374ae0

2 files changed +7 -7 lines changed

Top

Filter files…

- src
  - util.c
- tests
  - shtest

2 files changed +7 -7 lines changed

Search within code

src/util.c

```
@@ -312,13 +312,7 @@ static int jq_util_input_read_more(jq_util_input_state
*state) {
312 312         if (p != NULL)
313 313           state->current_line++;
314 314
315     -       if (p == NULL && state->parser != NULL) {
316     -         /*
317     -          * There should be no NULs in JSON texts (but JSON text
318     -          * sequences are another story).
319     -          */
```

```
320       -         state->buf_valid_len = strlen(state->buf);
321       -       } else if (p == NULL && feof(state->current_input)) {
      315 +       if (p == NULL && feof(state->current_input)) {
322   316           size_t i;
323   317
324   318           /*
```

tests/shtest

```
      @@ -880,4 +880,10 @@ $JQ -nf $d/prog.jq 2> $d/out && {
880   880   }
881   881   diff $d/out $d/expected
882   882
      883 + # CVE-2026-33948: No NUL truncation in the JSON parser
      884 + if printf '{}\x00{}' | $JQ >/dev/null 2> /dev/null; then
      885 +   printf 'Error expected but jq exited successfully\n' 1>&2
      886 +   exit 1
      887 + fi
      888 +
883   889   exit 0
```

Comments 0

Please sign in to comment.