radareorg / **radare2** Public

Code | Issues 773 | Pull requests 46 | Discussions | Actions | Projects

Commit 9236f44

jakelamberson authored 3 weeks ago · ✕ 48 / 52 · Verified

```
Fix #25650 - Command injection in curl PDB download ##crash

r_str_escape_sh assumes that the resulting string will be
surrounded by double quotes when consumed.
```

master (#25651) · 6.1.4

1 parent 37ed714 commit 9236f44

1 file changed +3 -3 lines changed

Top

Filter files…

libr/socket

socket_http.c

1 file changed +3 -3 lines changed

Search within code

libr/socket/socket_http.c

```
@@ -286,7 +286,7 @@ static char *socket_http_get_recursive(const char *url,
const char **headers, in
286 286             return NULL;
287 287         }
288 288         RStrBuf *sb = r_strbuf_new ("curl -s -D ");
289     -         r_strbuf_appendf (sb, "'%s' -o '%s' -L --max-redirs %u",
escaped_header_file, escaped_body_file, redirections);
    289 +         r_strbuf_appendf (sb, "\"%s\" -o \"%s\" -L --max-redirs %u",
escaped_header_file, escaped_body_file, redirections);
290 290         if (headers) {
291 291             const char **header = headers;
```

```
292  292                 while (*header) {
     @@ -300,12 +300,12 @@ static char *socket_http_get_recursive(const char
     *url, const char **headers, in
300  300                     free (body_file);
301  301                     return NULL;
302  302                 }
303      -               r_strbuf_appendf (sb, " -H '%s'", escaped_header);
     303 +               r_strbuf_appendf (sb, " -H \"%s\"", escaped_header);
304  304                 free (escaped_header);
305  305                 header++;
306  306             }
307  307         }
308      -       r_strbuf_appendf (sb, " '%s'", escaped_url);
     308 +       r_strbuf_appendf (sb, " \"%s\"", escaped_url);
309  309         char *command = r_strbuf_drain (sb);
310  310         free (escaped_url);
311  311         free (escaped_header_file);
```

Comments 0

Please sign in to comment.