

Commit c20aa27



RanMaoyi authored and JaylinYu committed on Dec 24, 2025 · ✖ 3 / 8



* FIX [auth] Fix crash in HTTP auth when using %u/%P with anonymous connections

Add NULL and empty string checks for req_data in auth_http.c:set_data().
Avoid calling strlen(req_data) for GET requests when no effective params
are built (e.g. username/password missing). Prevent remotely triggerable
SIGSEGV and broker DoS caused by HTTP authentication

Signed-off-by: Moi Ran <maoyi.ran@emqx.io>

main (#1394) · 0.24.11 ... 0.24.7

1 parent [dfa4b63](#) commit c20aa27

1 file changed +9 -7 lines changed

↑ Top ⚙

Filter files...

src/sp/protocol/mqtt

auth_http.c

1 file changed +9 -7 lines changed

Search within code ⚙

src/sp/protocol/mqtt/auth_http.c

```

@@ -240,13 +240,15 @@ set_data(
240 240
241 241     if (nni_strcasecmp(req_conf->method, "post") == 0 ||
242 242         nni_strcasecmp(req_conf->method, "put") == 0) {
243 -     if (req_data)
244 -         nng_http_req_copy_data(req, req_data, strlen(req_data));
245 -     } else {
246 -         size_t uri_len =
247 -             strlen(nng_http_req_get_uri(req)) + strlen(req_data) + 2;

```

```
248 - char *uri = nng_alloc(uri_len);
249 - sprintf(uri, "%s%s", nng_http_req_get_uri(req), req_data);
243 + if (req_data && req_data[0] != '\0') {
244 +     nng_http_req_copy_data(
245 +         req, req_data, strlen(req_data));
246 + }
247 + } else if (req_data && req_data[0] != '\0') {
248 +     const char *base_uri = nng_http_req_get_uri(req);
249 +     size_t      uri_len  = strlen(base_uri) + strlen(req_data) + 2;
250 +     char *      uri      = nng_alloc(uri_len);
251 +     snprintf(uri, uri_len, "%s%s", base_uri, req_data);
250 252     nng_http_req_set_uri(req, uri);
251 253     nng_free(uri, uri_len);
252 254 }
.....
↓
```

Comments 0



Please [sign in](#) to comment.