alibaba / xquic Public

Code Issues 40 Pull requests 10 Discussions Actions Security and

Commit 4764604

Sy0307 authored on Dec 12, 2025 · ✕ 3 / 4 · Verified

[+] Fix: Handle illegal STREAM frames in INIT and HSK packets (#524)

main (#524)

1 parent 108a34c commit 4764604

2 files changed +19 -0 lines changed

Top

Filter files…

- src/transport
  - xqc_frame.c
- tests/unittest
  - xqc_process_frame_test.c

2 files changed +19 -0 lines changed

Search within code

src/transport/xqc_frame.c

```
@@ -447,6 +447,16 @@ xqc_process_stream_frame(xqc_connection_t *conn,
xqc_packet_in_t *packet_in)
447 447         xqc_stream_t        *stream = NULL;
448 448         xqc_stream_frame_t  *stream_frame;
449 449
    450 +     if (packet_in->pi_pkt.pkt_type == XQC_PTYPE_INIT
    451 +         || packet_in->pi_pkt.pkt_type == XQC_PTYPE_HSK)
    452 +     {
    453 +         xqc_log(conn->log, XQC_LOG_ERROR,
    454 +                 "|illegal STREAM frame in %s packet, close with
PROTOCOL_VIOLATION|",
```

```
455 +                 xqc_pkt_type_2_str(packet_in->pi_pkt.pkt_type));
456 +         XQC_CONN_ERR(conn, TRA_PROTOCOL_VIOLATION);
457 +         return -XQC_EPROTO;
458 +     }
459 +
450 460         stream_frame = xqc_calloc(1, sizeof(xqc_stream_frame_t));
451 461         if (stream_frame == NULL) {
452 462             xqc_log(conn->log, XQC_LOG_ERROR, "|xqc_calloc error|");
```

tests/unittest/xqc_process_frame_test.c

```
    @@ -12,6 +12,7 @@
12  12
13  13    char XQC_TEST_ILL_FRAME_1[] = {0xff, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00};
14  14    char XQC_TEST_ZERO_LEN_NEW_TOKEN_FRAME[] = {0x07, 0x00};
    15  + char XQC_TEST_STREAM_FRAME[] = {0x0a, 0x00, 0x01, 0x00};
15  16
16  17
17  18    void
    @@ -31,6 +32,14 @@ xqc_test_process_frame()
31  32        ret = xqc_process_frames(conn, &packet_in);
32  33        CU_ASSERT(ret == -XQC_EPROTO);
33  34
    35  +     xqc_packet_in_t pi_stream_init;
    36  +     memset(&pi_stream_init, 0, sizeof(xqc_packet_in_t));
    37  +     pi_stream_init.pi_pkt.pkt_type = XQC_PTYPE_INIT;
    38  +     pi_stream_init.pos = XQC_TEST_STREAM_FRAME;
    39  +     pi_stream_init.last = pi_stream_init.pos + sizeof(XQC_TEST_STREAM_FRAME);
    40  +     ret = xqc_process_frames(conn, &pi_stream_init);
    41  +     CU_ASSERT(ret == -XQC_EPROTO);
    42  +
34  43        xqc_engine_destroy(conn->engine);
35  44    }
36  45
```

Comments 0

Please sign in to comment.