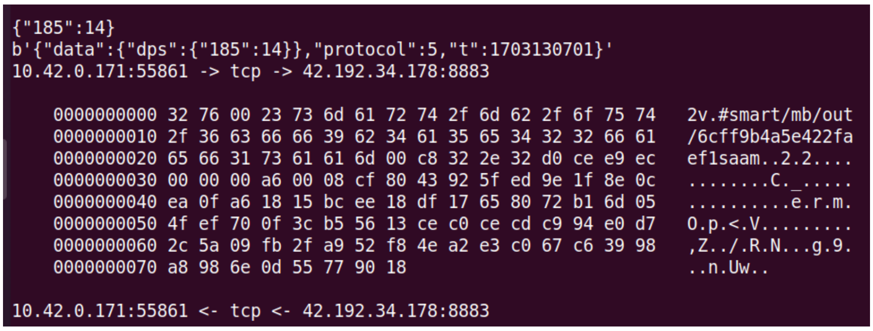
Tuya camera

Model: U6N

Firmware version: V3.2.5

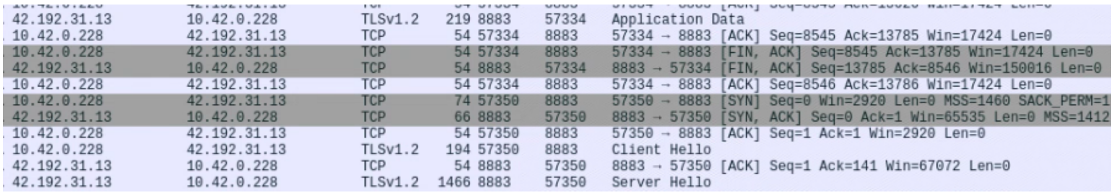
Product ID：6cff9b4a5e422faef1saam

After authentication, when sending commands to a camera via the Tuya Smart APP based on the MQTT protocol through a server, as shown in Figure 1, it was found that the device on the APP would temporarily go offline. At the same time, when capturing the communication packets between the device and the server, it was discovered that the device would actively send a FIN packet to terminate the current communication connection, as shown in Figures 2 and 3. This vulnerability leads to a denial of service for a period of time. The specific implementation involves triggering the execution of any control command to generate network traffic on the app side, then performing a man-in-the-middle attack between the APP and the server to decrypt the SSL/TLS packets. By reverse engineering the encryption algorithm, the original control commands are deduced. Subsequently, the control command ID and corresponding values are modified as shown in Figure 1. Afterward, new packets are generated according to the encryption and coding rules and sent to the server. The server then forwards these packets to the device side. Upon receiving these packets, the device behaves abnormally, resulting in the device going offline.



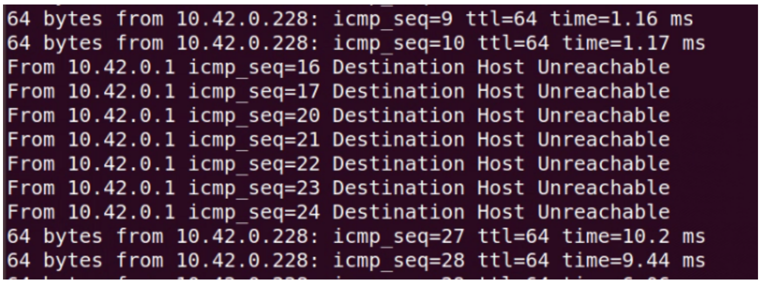
```
{"185":14}
b'{"data":{"dps":{"185":14}},"protocol":5,"t":1703130701}'
10.42.0.171:55861 -> tcp -> 42.192.34.178:8883

    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 66 66 39 62 34 61 35 65 34 32 32 66 61   /6cff9b4a5e422fa
    0000000020 65 66 31 73 61 61 6d 00 c8 32 2e 32 d0 ce e9 ec   ef1saam..2.2....
    0000000030 00 00 00 a6 00 08 cf 80 43 92 5f ed 9e 1f 8e 0c   ........C._.....
    0000000040 ea 0f a6 18 15 bc ee 18 df 17 65 80 72 b1 6d 05   ..........e.r.m.
    0000000050 4f ef 70 0f 3c b5 56 13 ce c0 ce cd c9 94 e0 d7   O.p.<.V.........
    0000000060 2c 5a 09 fb 2f a9 52 f8 4e a2 e3 c0 67 c6 39 98   ,Z../.R.N...g.9.
    0000000070 a8 98 6e 0d 55 77 90 18                           ..n.Uw..

10.42.0.171:55861 <- tcp <- 42.192.34.178:8883
```

Figure 1 The plaintext of a control command that can trigger an exception sending by App



```
42.192.31.13      10.42.0.228      TLSv1.2   219 8883   57334   Application Data
10.42.0.228       42.192.31.13     TCP        54 57334  8883    57334 → 8883 [ACK] Seq=8545 Ack=13785 Win=17424 Len=0
10.42.0.228       42.192.31.13     TCP        54 57334  8883    57334 → 8883 [FIN, ACK] Seq=8545 Ack=13785 Win=17424 Len=0
42.192.31.13      10.42.0.228      TCP        54 8883   57334   8883 → 57334 [FIN, ACK] Seq=13785 Ack=8546 Win=150016 Len=0
10.42.0.228       42.192.31.13     TCP        54 57334  8883    57334 → 8883 [ACK] Seq=8546 Ack=13786 Win=17424 Len=0
10.42.0.228       42.192.31.13     TCP        74 57350  8883    57350 → 8883 [SYN] Seq=0 Win=2920 Len=0 MSS=1460 SACK_PERM=1
42.192.31.13      10.42.0.228      TCP        66 8883   57350   8883 → 57350 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412
10.42.0.228       42.192.31.13     TCP        54 57350  8883    57350 → 8883 [ACK] Seq=1 Ack=1 Win=2920 Len=0
10.42.0.228       42.192.31.13     TLSv1.2   194 57350  8883    Client Hello
42.192.31.13      10.42.0.228      TCP        54 8883   57350   8883 → 57350 [ACK] Seq=1 Ack=141 Win=67072 Len=0
42.192.31.13      10.42.0.228      TLSv1.2  1466 8883   57350   Server Hello
```

Figure 2 Communication packets between the server and the camera



```
64 bytes from 10.42.0.228: icmp_seq=9 ttl=64 time=1.16 ms
64 bytes from 10.42.0.228: icmp_seq=10 ttl=64 time=1.17 ms
From 10.42.0.1 icmp_seq=16 Destination Host Unreachable
From 10.42.0.1 icmp_seq=17 Destination Host Unreachable
From 10.42.0.1 icmp_seq=20 Destination Host Unreachable
From 10.42.0.1 icmp_seq=21 Destination Host Unreachable
From 10.42.0.1 icmp_seq=22 Destination Host Unreachable
From 10.42.0.1 icmp_seq=23 Destination Host Unreachable
From 10.42.0.1 icmp_seq=24 Destination Host Unreachable
64 bytes from 10.42.0.228: icmp_seq=27 ttl=64 time=10.2 ms
64 bytes from 10.42.0.228: icmp_seq=28 ttl=64 time=9.44 ms
```

Figure 3 Devices within the local network will be unable to ping for a period of time after receiving a packet