Coap Server Crashed by sending multiple invalid requests

Short Description

Target Libcoap version: 4.3.1~1
Platform Os: Ubuntu 18.04 with kernel 6.1.21-x64v3-xanmode1
Discovered by: Zewen Shang Asset Research Group
Vulnerability Short Summary: An attacker can send the exact same packets in the same order to crash the coap server (implemented by using libcoap)
Vulnerability Impact: After the attack is successful, the server will crash immediately.

Summary of Relevant Files in This Report

scripts/attack1_coap.py: This script contains the attack code to crash the coap-server, the python version i used is 3.6.9
scripts/requirements.txt This script include all dependencies to run the script

Detailed Description

In order to trigger this crash, we build the simple coap_server and by using the command

```
dir: packages/framework-espidf2/
./install.sh
. ./export.sh

dir: packages/framework-espidf2/examples/protocols/coap_server
idf.py build
```

we also config the esp32 board to make sure it connect to the same wifi with the laptop it connected with and flash the code to the esp32 board by running the command

```
dir: packages/framework-espidf2/examples/protocols/coap_server
idf.py menuconfig
idf.py -p [port numebr] flash
```

Before running the script, the source and destination mac address need to be updated to the mac address of the wifi and the mac address of the board by changing the following two line of code:

```
frame[scapy.Ether].src ='wifi mac'

frame[scapy.Ether].dst = 'esp32 mac'
```

The destination ip of the packet will also need to be updated to the ip of esp32 board by updating the following line of code:

```
pkt[IP].dst = "esp32 ip"
```

2 packets must sent in sequence as specified in the python script attached. These two packets are all belongs to the Put Confirmable request.

After sending these two packets in sequence, the esp32 board will be rebooted as shown bellow:
Esp32 Reboot

and the following log of the server from idf.py openocd monitor indicates that the server has been crashed:

```
v:1 t:CON c:PUT i:c02a {591187a8deb9b733} [ Uri-Path:Espressif, Content-Format:text/plair
Guru Meditation Error: Core  0 panic'ed (LoadProhibited). Exception was unhandled.

Setting breakpoint at 0x400d9eb8 and returning...
0x400d9eb8: coap_handle_request_put_block at /home/asset/.platformio/packages/framework-e
```

Video of the attack

We also attached two videos to demonstrate the attack
Attack on openocd monitor
Attack on esp32 platformio