

🔑 main ▾ Vuln / Tenda AC21 / 10 /



xxy1126 -20220902 ...

on Sep 2 ⌚ History

..



readme.assets

3 months ago



readme.markdown

3 months ago



readme.markdown

Tenda AC21(V16.03.08.15) contains Stack Buffer Overflow Vulnerability

overview

- Manufacturer's website information: <https://www.tenda.com.cn/>
- Firmware download address: <https://www.tenda.com.cn/download/detail-3419.html>

product information

Tenda A21(V16.03.08.15), latest version of simulation overview:

AC21 升级软件 V16.03.08.15

立即下载

关联产品: AC21 更新日期: 2022/7/4

AC21V1.0升级说明
硬件版本: V1.0

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[11] = 0;
```

In function `set_qosMib_list`, it calls `strcpy(v8, s)`, `v8` is on the stack, so there is a buffer overflow vulnerability.


```
argv[4] = 00400  
snmp  
ifname wlan0 autoch select channel now!  
[tenda_autochannel_offset][11026] channel_offset=1  
ifname wlan0 ACS select channel:40  
Reaped pid = 5030  
argv[0] = httpd  
httpd
```

Yes:

```
***** WeLoveLinux*****
```

```
***** welcome to *****
```

```
[httpd][debug]-----webs.c,158  
httpd listen ip = 192.168.0.1 port = 80  
webs: Listening for HTTP requests at address 192.168.0.1
```