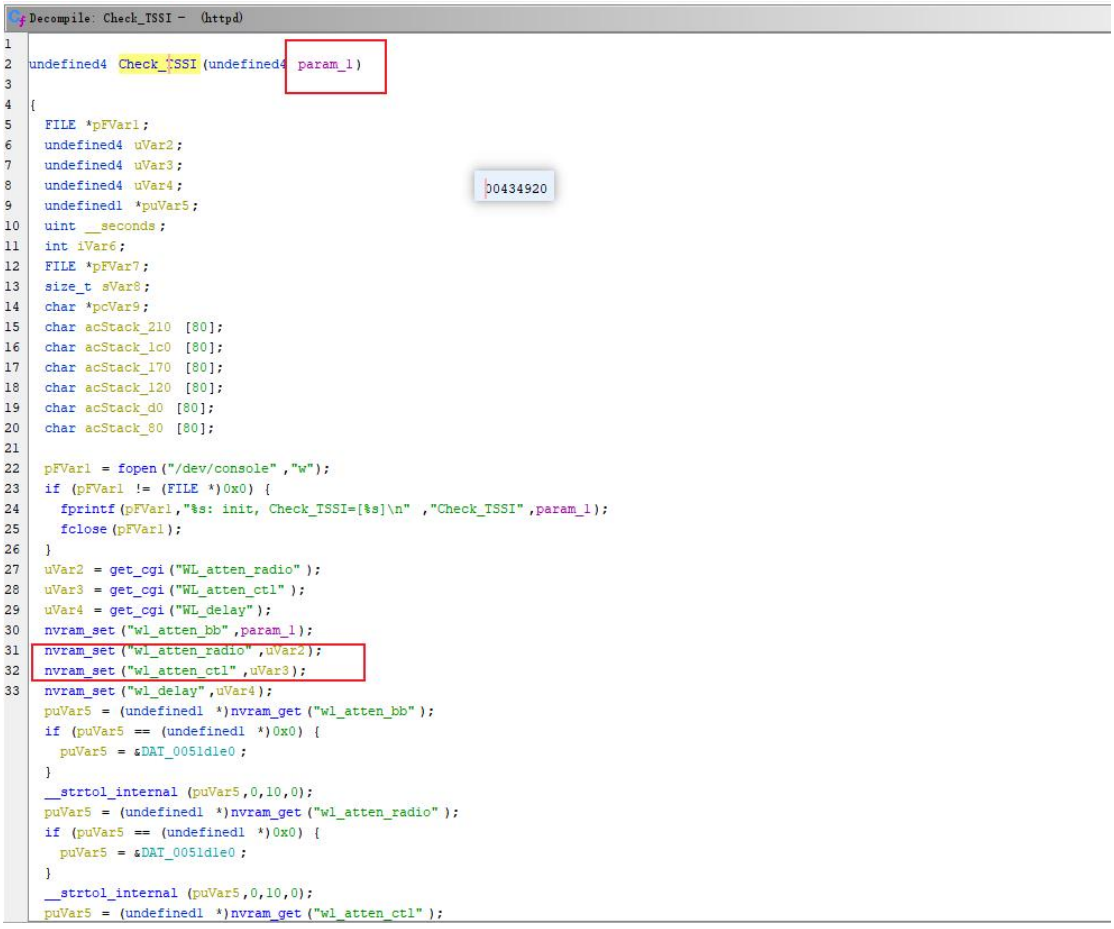
Vulnerability Description

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_atten_bb, WL_atten_radio, and WL_atten_ctl in the apply.cgi interface, thereby gaining shell privileges.

Code Analysis

In the function Check_TSSI, the parameter "param_1" is the WL_atten_bb parameter in the request, while the WL_atten_radio and WL_atten_ctl parameters also have command injection vulnerabilities.



```
Decompile: Check_TSSI - (httpd)
1
2  undefined4 Check_TSSI(undefined4 param_1)
3
4  {
5    FILE *pFVar1;
6    undefined4 uVar2;
7    undefined4 uVar3;
8    undefined4 uVar4;
9    undefined1 *puVar5;
10   uint __seconds;
11   int iVar6;
12   FILE *pFVar7;
13   size_t sVar8;
14   char *pcVar9;
15   char acStack_210 [80];
16   char acStack_1c0 [80];
17   char acStack_170 [80];
18   char acStack_120 [80];
19   char acStack_d0 [80];
20   char acStack_80 [80];
21
22   pFVar1 = fopen("/dev/console","w");
23   if (pFVar1 != (FILE *)0x0) {
24     fprintf(pFVar1,"%s: init, Check_TSSI=[%s]\n" ,"Check_TSSI",param_1);
25     fclose(pFVar1);
26   }
27   uVar2 = get_cgi("WL_atten_radio");
28   uVar3 = get_cgi("WL_atten_ctl");
29   uVar4 = get_cgi("WL_delay");
30   nvram_set("wl_atten_bb",param_1);
31   nvram_set("wl_atten_radio",uVar2);
32   nvram_set("wl_atten_ctl",uVar3);
33   nvram_set("wl_delay",uVar4);
     puVar5 = (undefined1 *)nvram_get("wl_atten_bb");
     if (puVar5 == (undefined1 *)0x0) {
       puVar5 = &DAT_0051d1e0;
     }
     __strtol_internal(puVar5,0,10,0);
     puVar5 = (undefined1 *)nvram_get("wl_atten_radio");
     if (puVar5 == (undefined1 *)0x0) {
       puVar5 = &DAT_0051d1e0;
     }
     __strtol_internal(puVar5,0,10,0);
     puVar5 = (undefined1 *)nvram_get("wl_atten_ctl");
```

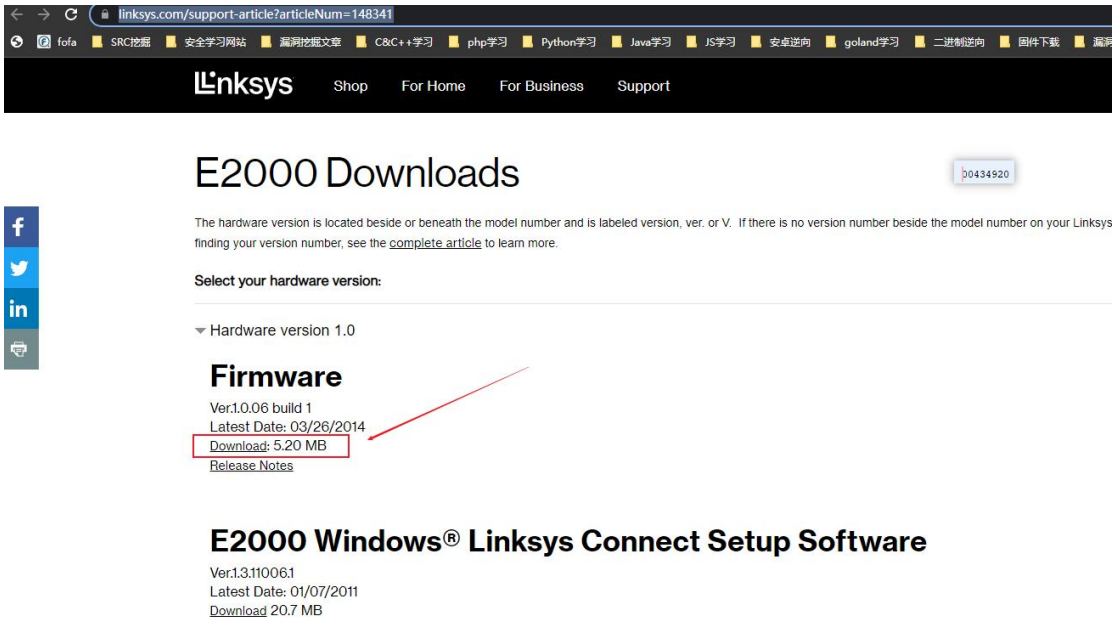
```
Decompile: Check_TSSI - (httpd)
  __strtol_internal (puVar5,0,10,0);
  puVar5 = (undefined1 *)nvram_get ("wl_atten_ctl");
  if (puVar5 == (undefined1 *)0x0) {
    puVar5 = &DAT_0051dle0;
  }
  __strtol_internal (puVar5,0,10,0);
  puVar5 = (undefined1 *)nvram_get ("wl_delay");
  if (puVar5 == (undefined1 *)0x0) {                    00434920
    puVar5 = &DAT_0051dle0;
  }
  __seconds = __strtol_internal (puVar5,0,10,0);
  pFVar1 = fopen ("/dev/console","w");
  if (pFVar1 != (FILE *)0x0) {
    fprintf (pFVar1,"%s: wl_atten_bb=[%s], wl_atten_radio=[%s], wl_atten_ctl=[%s]\n"   ,"Check_TSS...
    ,0,
            uVar2,uVar3);
    fclose (pFVar1);
  }
  iVar6 = validate_xss (uVar2);
  if ((iVar6 == 0) || (iVar6 = validate_xss (uVar3), iVar6 == 0)) {
    pFVar1 = fopen ("/dev/console","w");
    if (pFVar1 != (FILE *)0x0) {
      fprintf (pFVar1,"%s: parameter error!\n" ,"Check_TSSI");
      fclose (pFVar1);
    }
    return 0;
  }
  memset (acStack_1c0,0,0x50);
  sprintf (acStack_1c0,"wl atten %s %s %s",param_1,uVar2,uVar3);
  FUN_00475ca0 (acStack_1c0);
  pFVar1 = fopen ("/dev/console","w");
  if (pFVar1 != (FILE *)0x0) {
    fprintf (pFVar1,"%s: Will delay %d seconds\n" ,"Check_TSSI",__seconds);
    fclose (pFVar1);
  }
  if (__seconds != 0) {
    sleep (__seconds);
  }
  FUN_00475ca0 ("wl tssi > /tmp/get_tssi");
  memset (acStack_1c0,0,0x50);
  memset (acStack_d0,0,0x50);
  memset (acStack_d0,0,0x50);
  pFVar1 = fopen ("/tmp/get_tssi","r");
  if (pFVar1 == (FILE *)0x0) {
```

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

```
Decompile: FUN_00475ca0 - (httpd)
1
2  void FUN_00475ca0 (char *param_1)
3
4  {
5    FILE *__stream;
6
7    __stream = fopen ("/dev/console","w");
8    if (__stream != (FILE *)0x0) {
9      fprintf (__stream,"cmd: [%s]\n",param_1);
10     fclose (__stream);
11   }
12   system (param_1);
13   return;
14 }
15
```

Environment setup

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

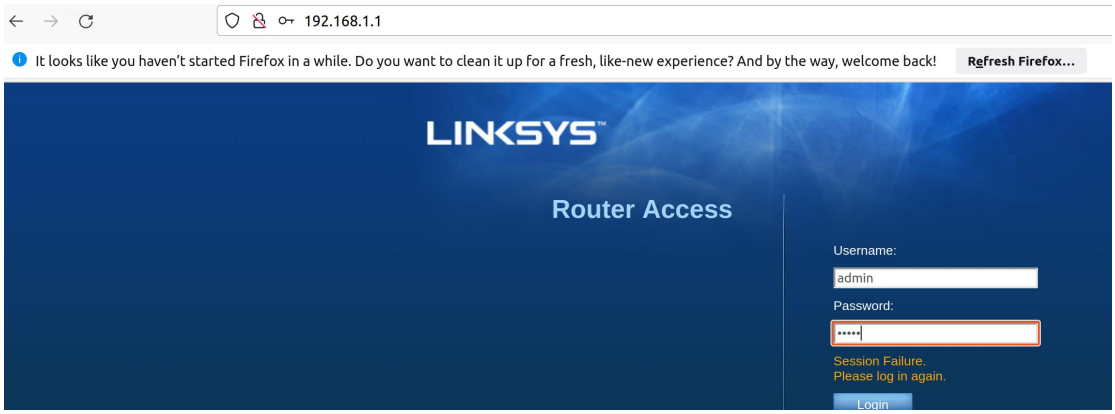


Set up the router environment through FirmAE.

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

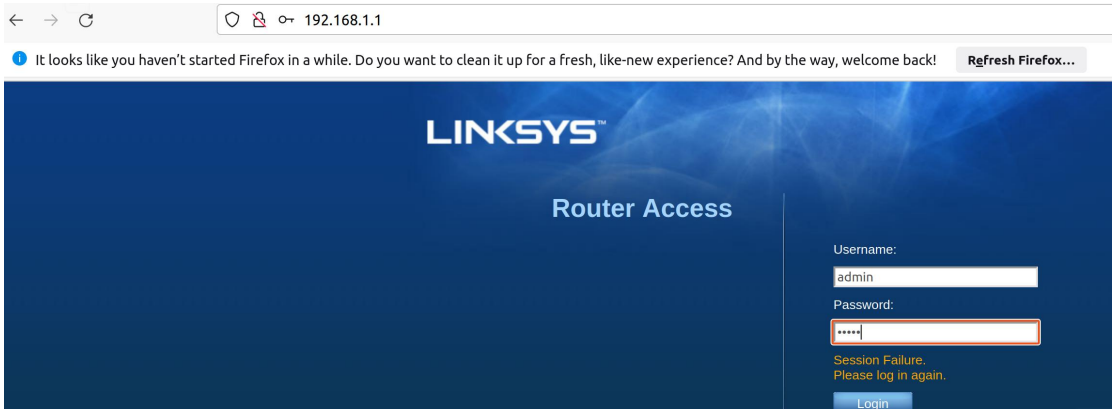
```
root@ubuntu:/FirmAE# ./run.sh -d Linksys /tmp/FW_E2000_1.0.06.001_US_20140310_code.bin
[*] /tmp/FW_E2000_1.0.06.001_US_20140310_code.bin emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
[*] /tmp/FW_E2000_1.0.06.001_US_20140310_code.bin already succeed emulation!!!

[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

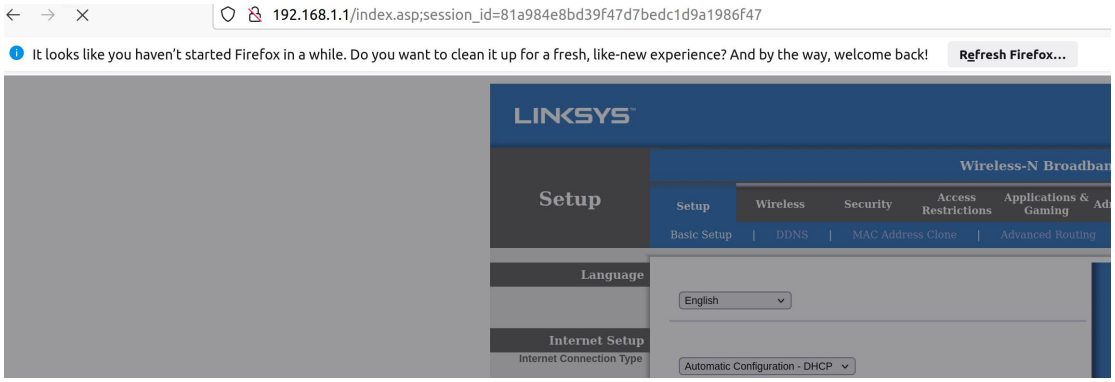


Vulnerability reproduction

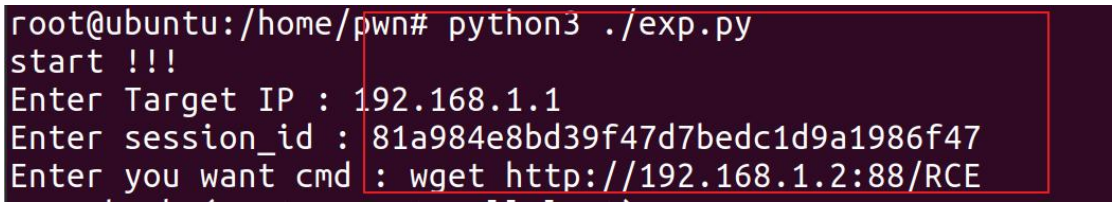
E2000 user：admin，password：admin



Obtain session ID after login



Run exp



Command injection successfully demonstrated.

Vulnerability Fix

Filter the characters ` $; | & from the parameters WL_atten_bb, WL_atten_radio, and WL_atten_ctl.