

main vuln / TOTOLINK / A7000R / 9 /



Darry-lang1 Add files via upload ...

on Jul 26 History

..



img

4 months ago



readme.md

4 months ago



readme.md







TOTOLink A7000R V9.1.0u.6115_B20201022 has a stack overflow vulnerability

Overview

- Manufacturer's website information: <https://www.totolink.net/>
- Firmware download address :
https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/171/ids/36.htm

Product Information

TOTOLink A7000R V9.1.0u.6115_B20201022 router, the latest version of simulation overview:

NO	Name	Version	Updated	Download
1	A7000R_Datasheet	Ver1.0	2020-08-07	
2	A7000R_Firmware	V4.1cu.3053_B20180329	2020-09-10	
3	A7000R_Firmware	V4.1cu.3382_B20180529	2020-09-10	
4	A7000R_Firmware	V4.1cu.4080_B20190530	2020-09-10	
5	A7000R_Firmware	V4.1cu.4154_B20191014	2020-09-10	
6	A7000R_Firmware	V9.1.0u.6115_B20201022(Transition version)	2020-12-30	

Vulnerability details

```

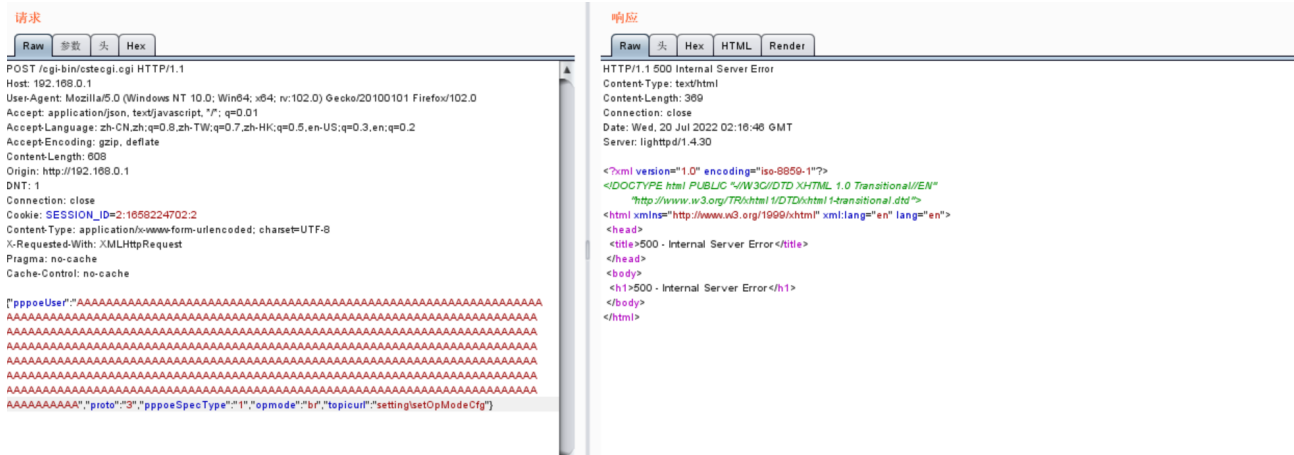
1 int __fastcall sub_42CC4C(int a1)
2 {
3     int Var; // $s1
4     int v3; // $s5
5     int v4; // $v0
6     int v5; // $s4
7     int JsonConf; // $v0
8     int v7; // $s2
9     _BYTE *v8; // $v0
10    int v9; // $v0
11
12    Var = websGetVar(a1, "opmode", "gw");
13    v3 = nvram_safe_get("opmode_custom");
14    v4 = websGetVar(a1, "wifiIdx_rpt", &word_438564);
15    v5 = atoi(v4);
16    nvram_set("opmode_custom", Var);
17    nvram_set_int("rt_mode_x", 0);
18    nvram_set_int("rt_sta_wisp", 0);
19    nvram_set_int("rt_sta_auto", 0);
20    nvram_set_int("wl_mode_x", 0);
21    nvram_set_int("wl_sta_wisp", 0);
22    nvram_set_int("wl_sta_auto", 0);
23    nvram_set_int("crpc_enable", 0);
24    if ( strcmp(Var, "gw") )
25    {
26        if ( !strcmp(Var, "br") )
27        {
28            nvram_set("wan_route_x", "IP_Bridged");
29            nvram_set_int("sw_mode", 3);
30            nvram_set_int("networkmap_fullscan", 0);
31            nvram_set_int("dhcp_enable_x", 0);
32            nvram_set("lan_proto_x", "1");
33            nvram_set("rt_guest_lan_isolate", &word_438564);
34            nvram_set("wl_guest_lan_isolate", &word_438564);
35        LABEL_19:
36            sub_424B84(a1);
37            sub_4262E0(a1);
38            sub_425FA0(a1);
39            goto LABEL_20;
40        }
41        if ( !strcmp(Var, "rpt") )

```

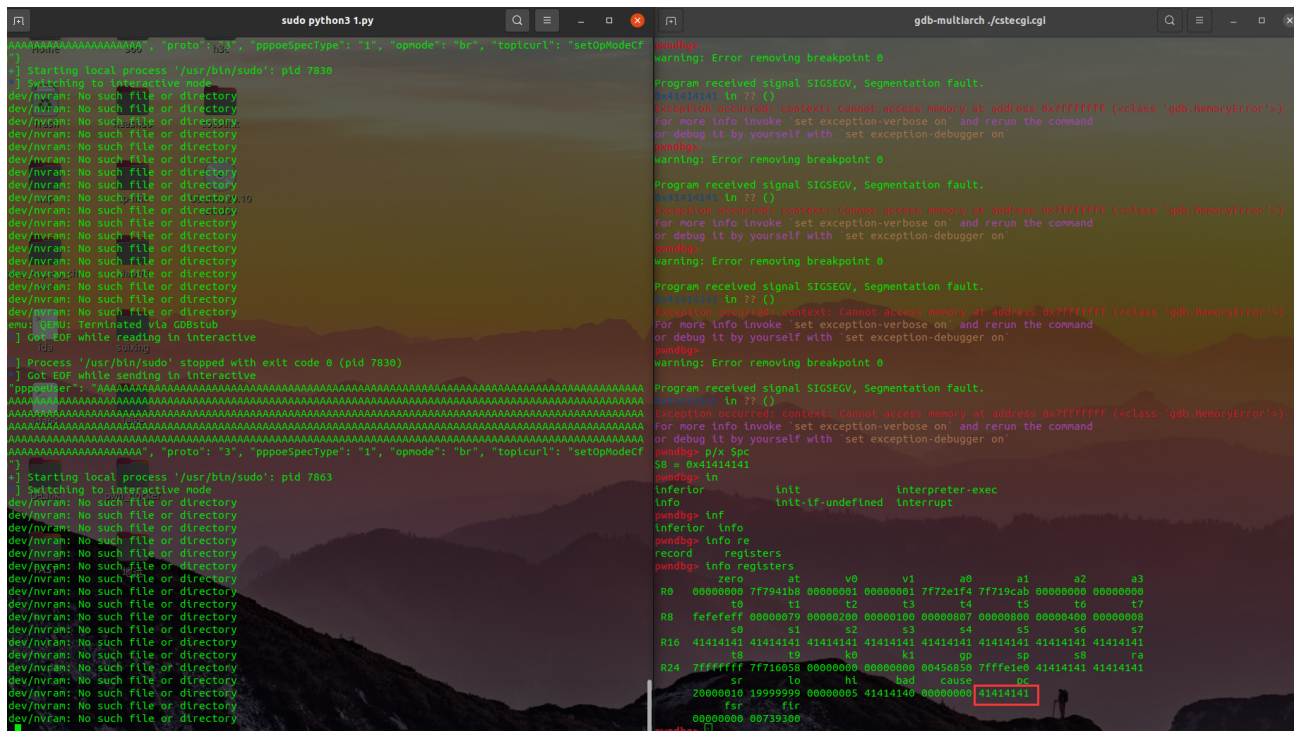
```

1 int __fastcall sub_424B84(int a1)
2 {
3     int String; // $v0
4
5     String = cJSON_CreateString("1");
6     cJSON_AddItemToObject(a1, "switchOpMode", String);
7     sub_423970(a1);
8     return 1;
9 }

```

The above figure shows the POC attack effect



As shown in the figure above, we can hijack PC registers.

```
BusyBox v1.24.2 (2020-12-02 18:57:43 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/ # ls -l
drwxrwxr-x  2 1000      1000      4096 Jul 19 22:40 bin
drwxrwxr-x  3 1000      1000      4096 Dec  2  2020 dev
drwxrwxr-x  2 1000      1000      4096 Dec  2  2020 etc
drwxrwxr-x  4 1000      1000      4096 Dec  2  2020 etc_ro
drwxrwxr-x  2 1000      1000      4096 Dec  2  2020 home
lrwxrwxrwx  1 1000      1000           7 Dec  2  2020 init -> sbin/rc
drwxrwxr-x  3 1000      1000      4096 Dec  2  2020 lib
drwxrwxr-x  3 1000      1000      4096 Dec  2  2020 lighttp
drwxrwxr-x  2 1000      1000      4096 Dec  2  2020 media
drwxrwxr-x  2 1000      1000      4096 Dec  2  2020 mnt
drwxrwxr-x  2 1000      1000      4096 Dec  2  2020 opt
drwxrwxr-x  2 1000      1000      4096 Dec  2  2020 proc
drwxrwxr-x  2 1000      1000      4096 Dec  2  2020 sbin
drwxrwxr-x  2 1000      1000      4096 Dec  2  2020 sys
drwxrwxr-x  2 1000      1000      4096 Dec  2  2020 tmp
drwxrwxr-x  9 1000      1000      4096 Dec  2  2020 usr
drwxrwxr-x  2 1000      1000      4096 Dec  2  2020 var
drwxrwxr-x  9 1000      1000      4096 Dec  2  2020 www

/ #
```

Finally, you can write exp to get a stable root shell without authorization.