

Nothing to see here

Protecting VPNs against decloaking

Till Maas
He/They





**Manager (Development and QE)
Network Management**

**Software Engineer
Nmstate
Network Ansible Role**

**Penetration Tester
Team lead, presenter**

FLOSS Contributor



TunnelVision (CVE-2024-3661): How Attackers Can Decloak Routing-Based VPNs For a Total VPN Leak

Network Security May 6





TunnelVision - What's required?

DHCP

Routing-based VPN

Virtual private network (VPN) is a [network architecture](#) for virtually extending a [private network](#) (i.e. any [computer network](#) which is not the public [Internet](#)) across one or multiple other networks which are either untrusted (as they are not controlled by the entity aiming to implement the VPN) or need to be isolated (thus making the lower network invisible or not directly usable).^[1]

A VPN can extend access to a private network to users who do not have direct access to it, such as an office network allowing secure access from off-site over the Internet.^[2] This is achieved by creating a link between [computing devices](#) and computer networks by the use of network [tunneling protocols](#).

It is possible to make a VPN secure to use on top of insecure communication medium (such as the public internet) by choosing a tunneling protocol that implements [encryption](#). This kind of VPN implementation has the benefit of reduced costs and greater flexibility, with respect to dedicated communication lines, for [remote workers](#).^[3]


```
# ip route show
```

```
# default means 0.0.0.0/0
```

```
default via 192.168.98.23 dev wlp9s0 proto dhcp src 192.168.98.245 metric 600
```

```
192.168.98.0/24 dev wlp9s0 proto kernel scope link src 192.168.98.245 metric 600
```


old

default means 0.0.0.0/0

default via 192.168.98.23 dev wlp9s0 proto dhcp src 192.168.98.245 metric 600

192.168.98.0/24 dev wlp9s0 proto kernel scope link src 192.168.98.245 metric 600

new, destinations to use the VPN for

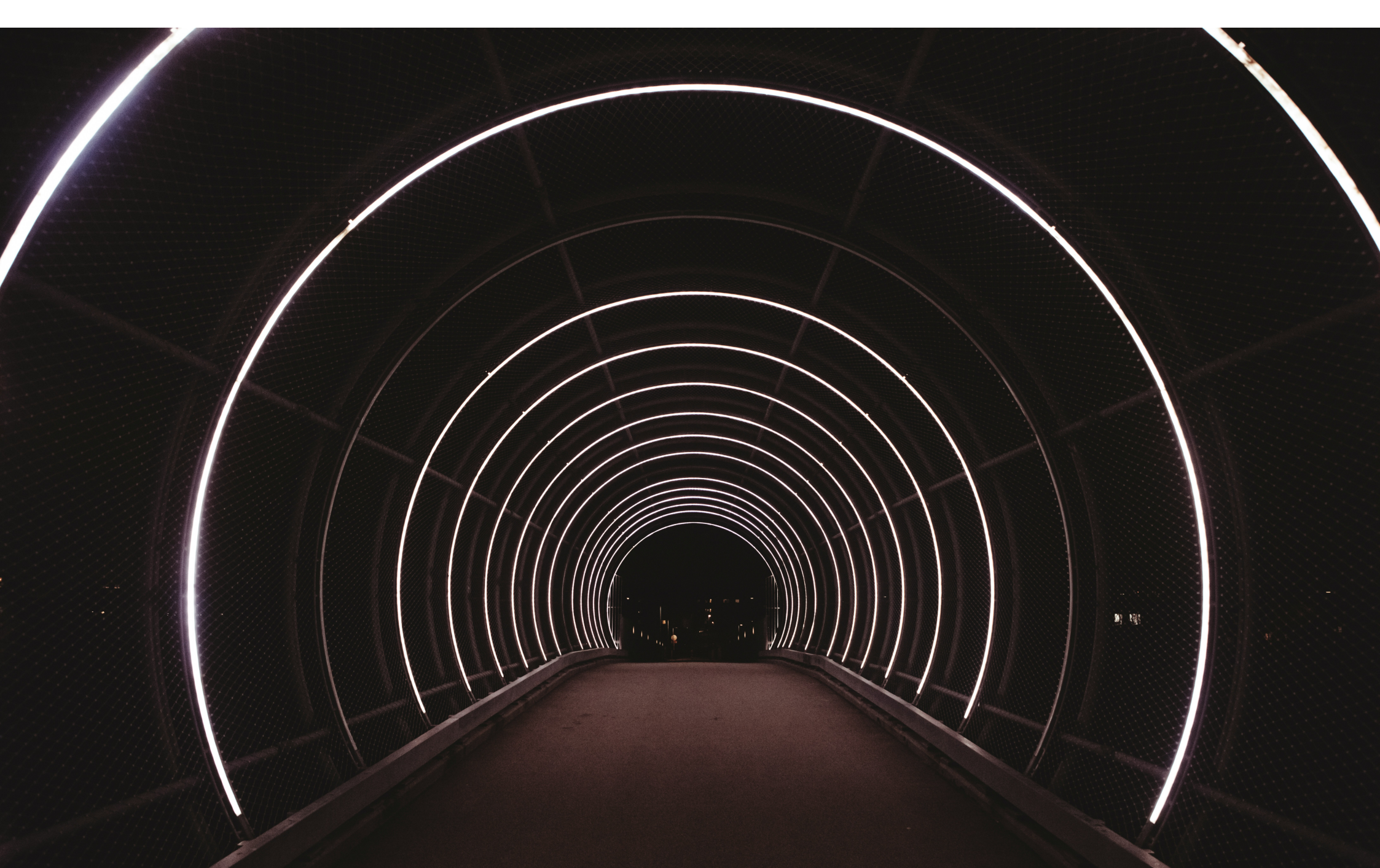
10.0.0.0/8 via 10.42.23.1 dev tun0 proto static metric 50

10.42.23.0/24 dev tun0 proto kernel scope link src 10.39.192.10 metric 50

new, routes to access the VPN server (192.168.55.1)

192.168.98.23 dev wlp9s0 proto static scope link metric 50

192.168.55.1 via 192.168.98.23 dev wlp9s0 proto static metric 50



DHCP Option 121 - Classless Static Route Option for DHCP


```
# destinations to use the VPN for  
10.0.0.0/8 via 10.42.23.1 dev tun0[...]  
10.42.23.0/24 dev tun0[...]
```

```
# The attack
```

```
10.0.1.0/24 dev wlp9s0 proto dhcp[...]  
10.0.2.0/24 dev wlp9s0 proto dhcp[...]  
10.0.3.0/24 dev wlp9s0 proto dhcp[...]  
[...]
```







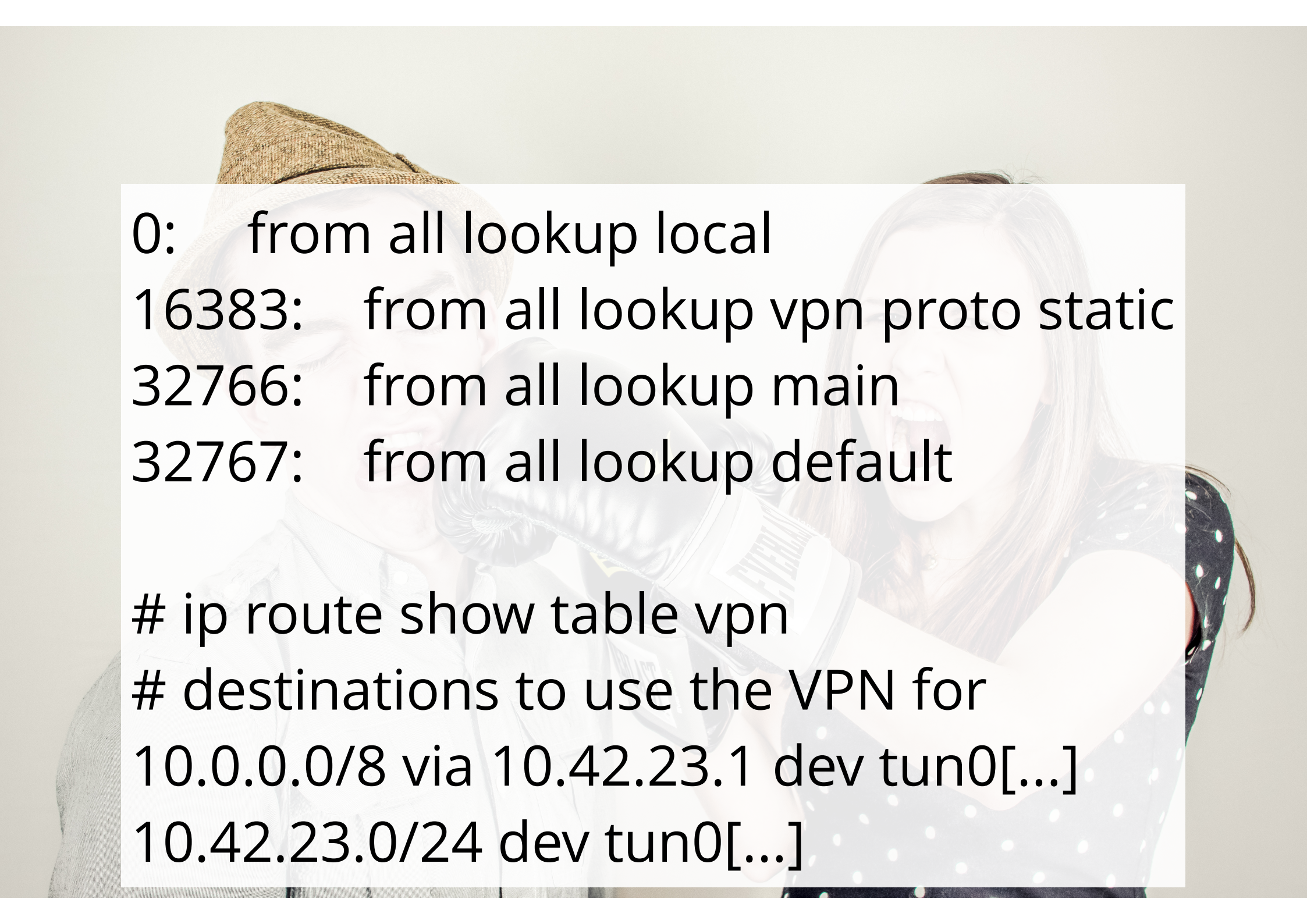
```
# ip rule show
```

```
# format: priority: policy
```

```
0:    from all lookup local
```

```
32766:  from all lookup main
```

```
32767:  from all lookup default
```


A man wearing a tan hat and a woman with long hair are looking at a laptop screen. The man is pointing at the screen with his right hand. The woman is looking at the screen with a surprised expression. The background is a plain, light-colored wall.

0: from all lookup local
16383: from all lookup vpn proto static
32766: from all lookup main
32767: from all lookup default

```
# ip route show table vpn  
# destinations to use the VPN for  
10.0.0.0/8 via 10.42.23.1 dev tun0[...]  
10.42.23.0/24 dev tun0[...]
```




Zeroday

Assigned CVE identifiers

Our findings were tracked by CERT/CC under the identifier VU#563667. Our attacks got assigned the following Common Vulnerabilities and Exposures (CVE) identifiers:

- CVE-2023-36672: LocalNet attack resulting in leakage of traffic in plaintext. The reference CVSS score is 6.8.
- CVE-2023-35838: LocalNet attack resulting in the blocking of traffic. The reference CVSS score is 3.1.
- CVE-2023-36673: ServerIP attack, combined with DNS spoofing, that can leak traffic to arbitrary IP address. The reference CVSS score is 7.4.
- CVE-2023-36671: ServerIP attack where only traffic to the real IP address of the VPN server can be leaked. The reference CVSS score is 3.1.

TunnelCrack - <https://tunnelcrack.mathyvanhoef.com/details.html>



DHCP Option 33 - Static Route Option

DHCP Option 249 - Microsoft Classless Static Route Option



More Zerodays



IPv6



```
nmcli connection modify MY_VPN_CONNECTION_NAME  
  ipv4.route-table 75  
  ipv4.routing-rules "priority 32000 from all table 75"  
  ipv6.route-table 75  
  ipv6.routing-rules "priority 32000 from all table 75"
```


A man with a beard is holding a piece of cardboard with handwritten text. The text on the sign reads: "ADVICE - \$.50", "GOOD ADVICE - \$2.00", and "and jokes for free". The man is wearing a tan jacket. The background is blurred, showing an outdoor setting.

ADVICE - \$.50
GOOD ADVICE - \$2.00
and jokes for free

routed VPNs make your routing table part of the VPN configuration
Secure users don't let DHCP (and SLAAC and DNS) change their VPN configuration
CVEs might be too specific
CVEs might be too broad



**Still some attack vectors open in NetworkManager
Make policy routing the default
Documentation**



What are your questions?



Please provide feedback via pretalx

Sources:

Ryan McGuire - <https://gratisography.com/>

Jakob Soby - https://unsplash.com/de/fotos/rot-weisser-tunnel-mit-rotem-teppich-RjPG_LVmiQ

Tima Miroshnichenko - <https://www.pexels.com/photo/a-blindfolded-woman-6608257/>

<https://www.leviathansecurity.com/blog/tunnelvision>

<https://tunnelcrack.mathyvanhoef.com/>

https://en.wikipedia.org/wiki/Virtual_private_network