black hat

Bypassing Tunnels: Leaking VPN Client Traffic by Abusing Routing Tables

Nian Xue, Yashaswi Malla, Zihang Xia, Christina Pöpper, and Mathy Vanhoef



#BHEU @BlackHatEvents

Contributions

We make VPN clients leak traffic

- > By manipulating the client's routing table
- > Attacks are independent of the crypto protocol

Tested 67+ VPN clients

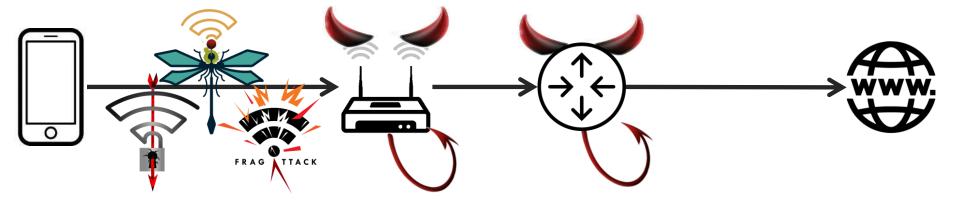
- > >248 experiments \rightarrow 66% attack success
- > Every VPN is vulnerable on at least one OS

→ Widespread design issues!

Usage of VPNs: watch videos from other country



Usage of VPNs: protect your traffic



- > Identify website visits: IP address, plaintext DNS, SNI,...
- > Attack TLS: no cert check, sslstrip, academic attacks,...

Usage of VPNs: protect your traffic



- > Defend against untrusted Wi-Fi & compromised core routers
- > Research goal: can we trick the client into leaking packets?
 - » Yes, by manipulating the client's routing table \rightarrow ~66% vulnerable!
 - » Attacks are independent of the crypto protocol





\$ ip route # Simplified ouput
1 default via tun0

1. By default, send packets over tun0 = over the VPN tunnel



\$ ip route # Simplified ouput
1 default via tun0
2 192.168.1.0/24 via eth0

1. By default, send packets over tun0 = over the VPN tunnel

2. LocalNet exception: local network is directly accessible



\$ ip route # Simplified ouput
default via tun0
1 192.168.1.0/24 via eth0
3 2.2.2.2 via eth0

1. By default, send packets over tun0 = over the VPN tunnel

- 2. LocalNet exception: local network is directly accessible
- 3. ServerIP exception: avoid re-encryption of VPN packets

We assume secure DNS behavior



\$ cat /etc/resolv.conf
nameserver 6.6.6.6

Can't trust the network's DNS server

We assume secure DNS behavior



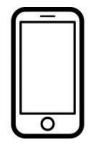
\$ cat /etc/resolv.conf
nameserver 2.2.3

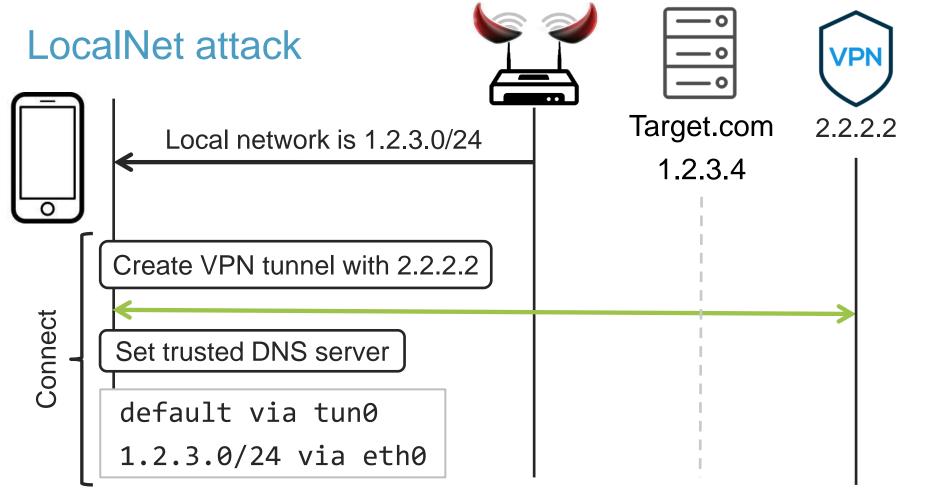
Can't trust the network's DNS server

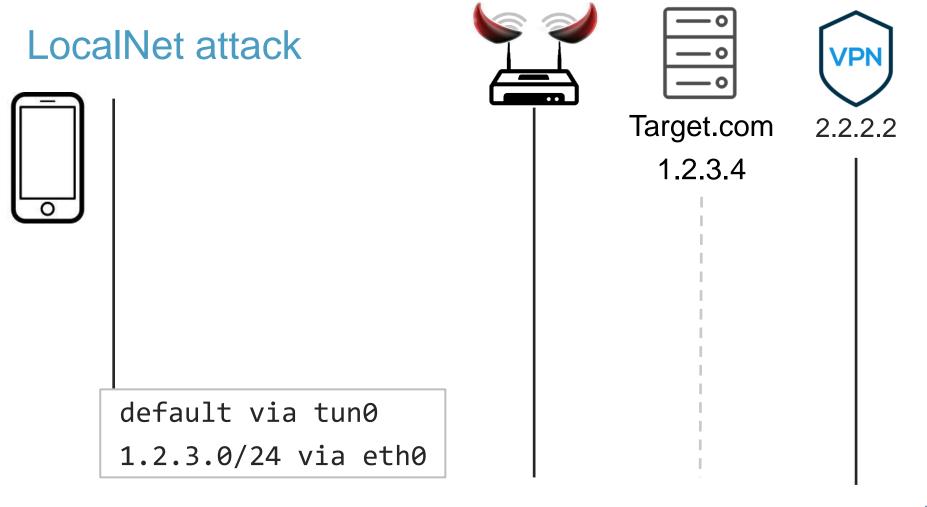
- 1. Once connected, VPN client sets a trusted DNS server
- 2. DNS is sent through the VPN tunnel
 - + we assume other routing-based attacks are prevented

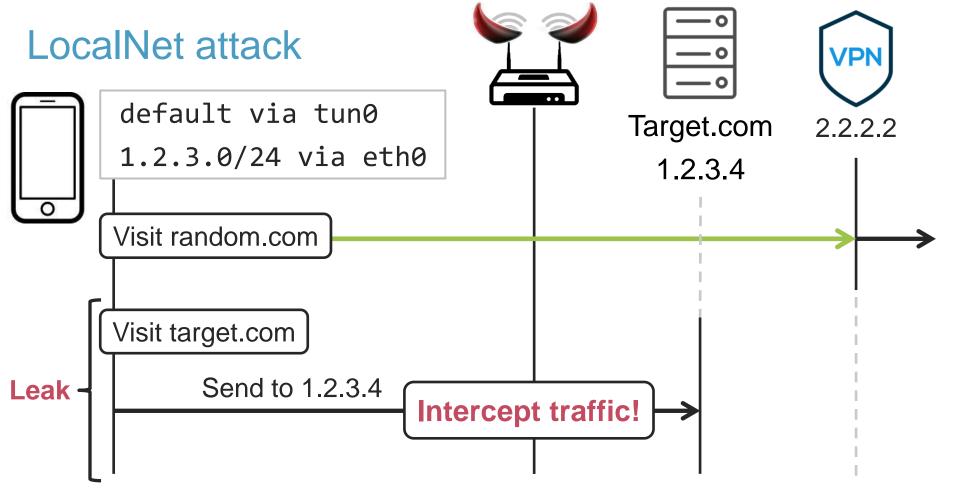
LocalNet attack











		k: 195		ments	VALUATED USENIX Association AVAILABLE	EVALUATED USENIX ASSOCIATION REPRODUCED
Version Pro- Prese Weak Workshow OS Built is UPN Prese Windows Windows OS Built is UPN Prese Android Windows Prese Model Android Android Prese Android Android Android Prese Line 20220.10 Prese Android 11 Prese Line 20229.10 Prese 4.01 Prese Jense 2022.9.1 Prese 4.01		Class	OS	Version Number	LAN Setting Default LAN Acco	Result ess
Any Vr. Windo 1.0.8 Avira Phantom Pree Windows Best VPN Pree macOS Paid Windows		Free	Windows	Windows 10 Pro	No N/A	×
Betternet Paid i08 5.2. Paid i08 5.2. Paid Android 6.2.0 Free Windows 4.10.040 Free Linux 4.10.040		Free	Windows	Windows 11 Pro	No N/A	×
Cisco AnyConnect Free macOS 4.10.04 Free iOS 50.000 Free Android 50.000 Paid Windows 5.9.1.16	OS Duilt in VDN	Free	macOS	Ventura 13.0.1	No N/A	×
Clario VPN Paid macOS 5.9.1.10 Paid iOS 1.9.22 Paid Android 1.9.26.42 Paid Windows 8.3.7.97		Free	iOS iOS 16.1.1		No N/A	×
Paid Linux 1.3.4 CyberGhost Paid macOS 8.3.9.1 Paid iOS 8.4.0 Paid Android 8.6.17.1	4 167 0	Free	Android	Android 8.1.0	No N/A	 ✓
Paid Windows 12.37. Paid Linux 3.36 ExpressVPN Paid macOS 11.12. Paid iOS 11.70. Paid iOS 11.06.		Free	Android	Android 12	No N/A	
Fast VPN-solo anlimited proxy Free iOS 2.2.4 Paid Windows 3.4.0.1 Fast VPN Paid macOS 3.0.0 by Namecheap Paid macOS 3.7.0 Paid Android 3.4.2 3.4.0	0	Free	Windows	2022.10.106.0	No N/A	
Free VPN Free MacOS 3.884 by Free VPN.org Free iOS 3.879 Free Android 3.9	4	Free	Linux	2022.9.591	No N/A	× 1
Paid Windows 50.00 Paid macOS 5.1.3 Paid iOS 5.1.4 Paid iOS 5.1.4 Paid Android 5.1.4(1)	³ 95) 1.1.1.1	Free	macOS	2022.10.107.0	No N/A	\bigtriangleup
Free / Paid Windows 3.14.0 Free / Paid Linux 0.9.2. Hide.me VPN Free / Paid macOS 4.7.1 Free / Paid iOS 4.111 Free / Paid iOS 4.111	2	Free	iOS	6.16	No N/A	×
Paid Windows 5.21.67 Paid Linux 0.5 HideMyAss Paid macOS 5.4.7 Paid noCOS 5.100 Paid Android 5.58.65	7 00	Free	Android	6.17	No N/A	V
Fine Mindows 2.06.05 Fine Windows 2.103 Hotspot Shield Fine macOS 5.30610 Fine Android 9.9.0	8 023 0				1	
Paid Windows 4.1.2.1 IPVanish Paid macOS 3.3.0(67 Paid iOS 4.4.0 Paid iOS 4.0.3	22 Yes Yes X Paid Windows 4799 No N/A X TorGuard Paid macOS 0 No N/A X Paid 30S	4.8.13 No NA X 4.8.13 No NA X 4.8.13 No NA X 2.2.8 No NA X 1.60.9 No NA X	Pice Android L0.20220316 Pice Windows 73.0.2674 XVPN Pice macOS 73.1.0.2791 Pice iOS 31.3	6 No NA V No NA V No NA X		
Paid Windows 2022.5 Paid macOS 2022. Mailvad Paid Linux 2022. Paid iOS 2022. Paid Android 2022.	5.0 Yes No △ 5 Yes No △ 5 Yes No △ 7 TouchVPN Free macOS 7 No N/A ¥	2.02.274 No VA X 2.56.158 No VA X 4.4.1 No VA X 2.0.8 No VA X	Prec KAS Free Android 180.2778 ¥ always vulnenkle, ¥ vulnenkle by default LAN-Access-Setti ♥ vulnenkle by using special use IP addresses ✔ always secure, ✔ secure by default LAN-Access-Setting, △ local traffic blocket	No N/A V ting		16

ARTIFACT

ARTIFACT

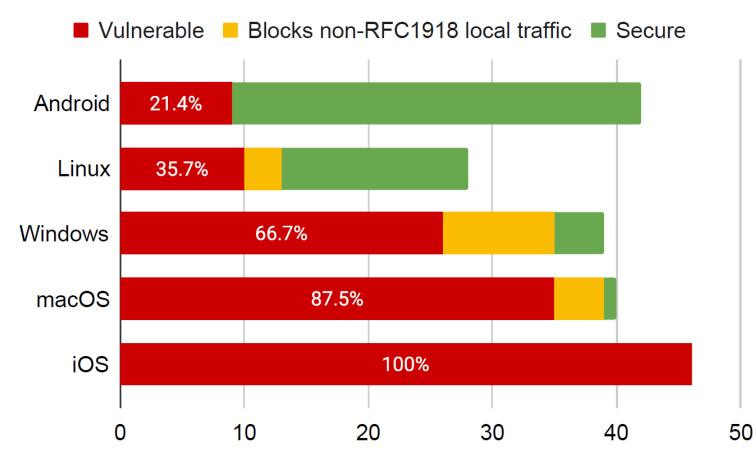
ARTIFACT

								np o				FUNCTIONAL	REPRODUCED
Table 1 V v view OS Built-in V	Fine Fine Fine Fine Fine	Windo Windon macO0 iOS Android Android Window Linu	Version Number Windows 10 Pro Windows 11 Pro Ventura 13.0.1 iOS 16.1.1 Android 8.1.0 Android 12 2022 10.106.0 2022 9.501	terent VPN clients. LAN Setting Result Default LAN Access No: N/A X No: N/A X No: N/A X	Network Manager Pine Pine Linn Linn Pine OpenVPN Grome Pine Linn Linn Pidd Mark Pidd Linn NontVPN Pidd mark Linn	t 1.8.2 No N t 1.8.12 No N t 1.8.18 No N ws 7.2.2.0 No N t 1.0.0 No N	A X A V A V TunnelBear A A Tunnelblick	Paid Windows Paid macOS Paid iOS Paid Adroid Fite macOS Fite MacOS	4.6.1 No N/A Δ 4.1.8 No N/A X 4.2.3 No N/A X 3.6.8 No N/A X 3.8.7 m No N/A X 1.10.0 No No X			1	
Li Any Vi Avira Phaniton Best VPN Besternet Cisco AnyCon Clario VPN CyberGhost	Free Free Free Free Free Free Paid Paid Paid Free Free Free Free Free Free Free Paid Paid Paid Paid Paid Paid Paid Paid	ma Windows macOS Windows macOS iOS Android Windows Linux acOS iOS Android Windows Linux Linux macOS iOS Android Windows Linux Linux macOS iOS	2022 10.1070 6.16 6.17 1.0.8 1.0.8 1.0.26 4.10.20405 4.10.20405 4.10.20405 4.10.20405 4.10.20405 5.00.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.000247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247 5.0.20405 5.0.00247	Exp	ressVPN	Pa Pa Pa	aid aid aid aid aid	Window Linux macOs iOS Androi	5	12.37.0 3.36 11.12.0 11.70.0 10.63.2		Yes Yes No N/A Yes Yes Yes Yes Yes Yes	
Express VPN Past VPN-sole anlimited prov Fast VPN by Namecheag Pree VPN by Free VPN	y Pree Paid Paid Paid Paid Free Free	Android Windows Linux macOS iOS Android iOS Windows macOS iOS Android macOS iOS Android	8617.1164 12.37.0 3.36 11.12.0 11.70.0 10.63.2 2.2.4 3.40.0 3.9.0 3.7.0 3.4.2 3.884 3.879 3.9		N Proxy N iPhone	Master	Free		iOS		2.1.5	No N/A	ŧ
Goose VPN Hide.me VPN HideMyAss	Paid Paid Paid Paid Pree / Paid Pree / Paid Pree / Paid Pree / Paid Paid Paid Paid Paid	Linux macOS iOS	\$00.9 \$.13 \$.14 \$.1.4(195) 3.14.0 0.92 4.7.1 4.11.0 3.10.0 \$21.6744 0.5 \$.4.7 \$.1.0 \$.1.6 \$.1.6 \$.1.4(195) \$.1.10 \$.1.4(195) \$.1.4(1	Yes No A No N/A A No N/A X No N/A X	Star VPN Free Window Free incc Free iOS Free Andre Paid Window Paid Mucc Paid Andre Paid Andre	S 2.11.0 No N 3.60 No N id 1.8 No N ws 2.62.0 No N 2.60 No N id 2.3.3.6 Yes N	A X A X Windscribe built-in A X A X A X Windscribe 3rd-pa	Pree iOS Pree Android rty Pree Linux	11113911 No No P 25.17 Yes No A 25.17 Yes No A 25.17 Yes No A 33.1003 Yes No Image: A 25.17 Yes No Image: A 25.17 Yes No Image: A 25.17 Yes No Image: A				, in the second s
Hotspot Shield IPVanish Mullvad	Free	Vindows macOS iOS Android Windows macOS iOS Android Windows macOS Linux iOS Android	2.10.8 2.10.8 5.3.061028 7.9.0 9.9.0 4.1.2.122 3.3.0(67479) 4.4.0 4.0.3 2022.5.0 2022.5 2022.5 2022.2 2022.3	100 100 No NA No NA No NA No NA Yes No	Super VPN Tree ADS Secure VPN Muter Free Andre TLS Tunnel Free Andre Dial Mail Line TarGuard Paid Mail TarGuard Paid Mail TarGuard Paid Mail TarGuard Paid Mail TouchVPN Free Wind TouchVPN Free Andre	id 1.6.2 No N N id 50.5 No N N 4.8.13 No N N 4.8.13 No N 4.8.13 No N 4.8.13 No N 4.8.13 No N id 1.60.9 No N Ne N N N N N N N N N N N N N 4.8.14 No N N N N N N N N N N N N N N N N N N	A V A X A X A X A X A X A X XVPN A X X always v alnet	Pree Windows Pree Linux Pree macOS Pree iOS Pree iOS Pree Mindows Pree macOS Pree iOS Pree iOS Pree iOS Pree iOS Pree iOS Pree Android	ilways secure,				17

LocalNet attack: 195 experiments



LocalNet attack: summary





=	mathy@zbook-mathy:~/research/netsec/vpnproject-main/vpn_tester	- " ×
File Edit View Search Terminal Help		
[mathy@zbook-mathy	<pre>vpn_tester]\$</pre>	
🅢 🛅 🕘 🗑 Documents 💽 mathy@z	🔞 🎯 🌈 vpn_teste 🌈 The Wires 🕐 SimpleScr 🥐 🕯 🐇 1	ē ≎ (¢ 22:17

Selected special cases



Some clients block traffic to local network

- > Problem when local network uses public IPs
- > Traffic to these public IPs gets blocked!



VPN Proxy Master for iPhone (and others)
DNS server returns private-use IP addresses
VPN server forwards traffic to real IP address

The iOS case



Prevent attacks by setting includeAllNetworks=True

- > And excludeLocalNetworks=False on iOS ≥ 14.2
- > Causes reliability issues, vendors hesitant to enable this

Result is that iOS remains less secure

- Context: VPNs on iOS were already known to leak traffic in certain scenarios.
- > E.g., OS traffic may leak, leaks when switching networks,...

We were warned in the past...

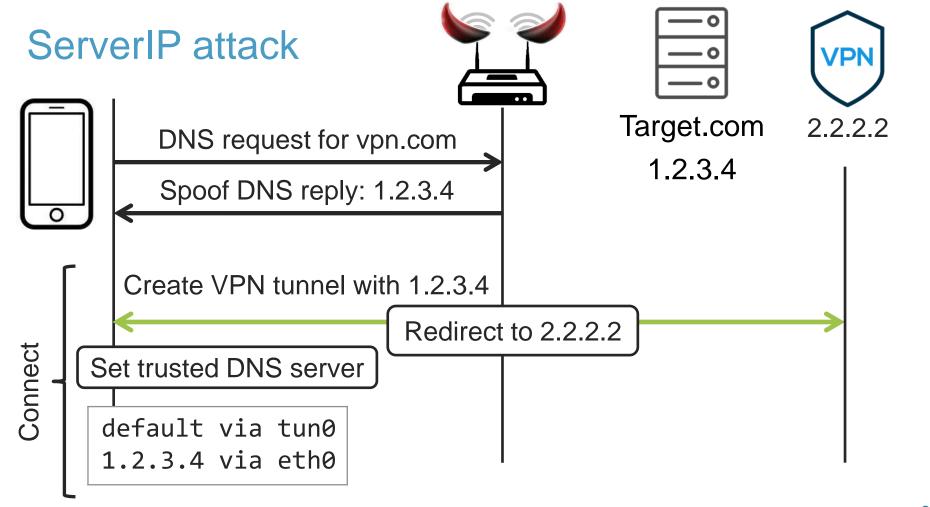
Andrew Ayer: <u>Hardening OpenVPN for DEF CON</u> (2015)

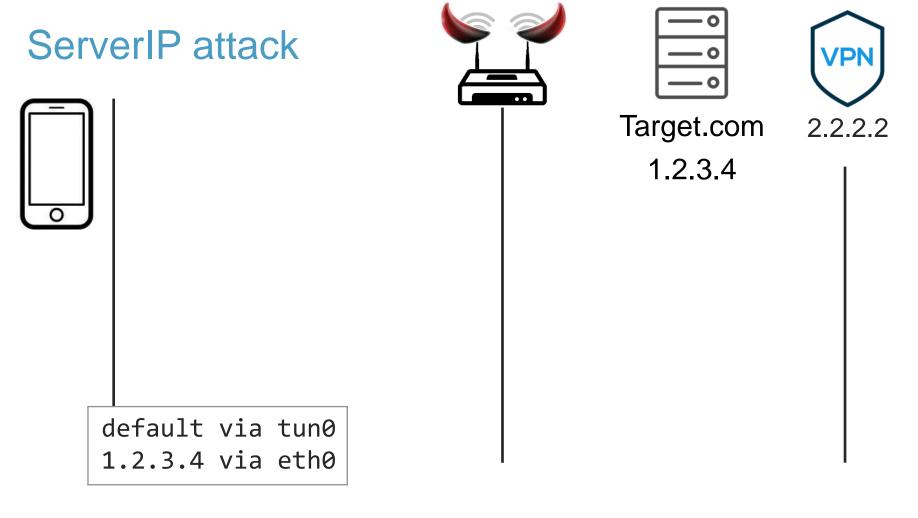
- > Guide for OpenVPN on Linux
- > Essentially suggested the risk of LocalNet attacks!

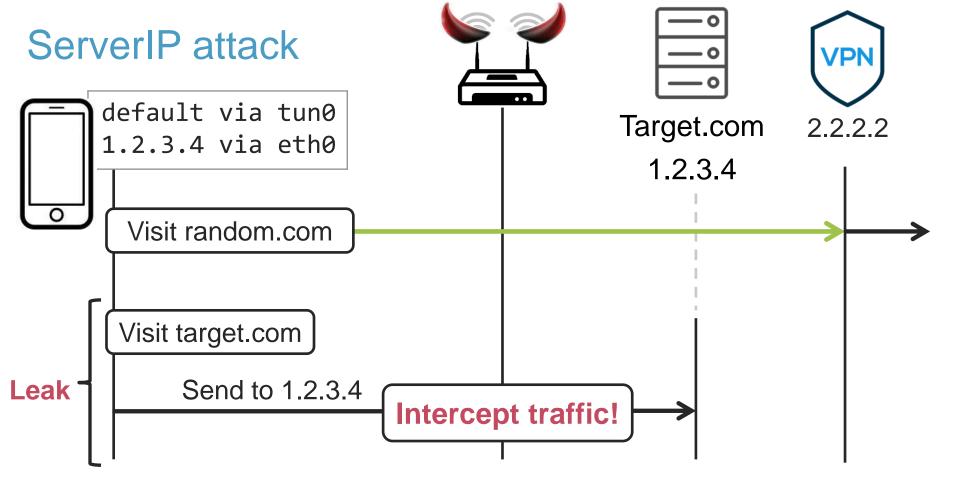
Unclear how widespread this issue (already) was at the time

- > VPN clients were not systematically tested → vendors were not warned, so clients never were not audited either
- > Using domain names would still enable ServerIP attacks...









ServerIP attack: 53 experiments

- > Many built-in clients are affected (Windows, macOS, Linux)
- > Legacy built-in VPN on Android 11 and below was affected
- > Most iOS/Android apps not vulnerable

Impact: can leak traffic to single IP address

- > Can target the DNS server set by the VPN client \odot
- > Or repeat the attack for different IPs...



mathy@mathy-VirtualBox:~/vpn_tester\$
mathy@mathy-VirtualBox:~/vpn_tester\$
mathy@mathy-VirtualBox:~/vpn_tester\$
mathy@mathy-VirtualBox:~/vpn_tester\$

Defenses

LocalNet attack: disable local network access when it's using public IP addresses.

> Or allow local network access when using 192.168.* or alike

ServerIP Attack: send all traffic over VPN, except packets generated by VPN process

- > On Linux, you can use fwmark (policy-based routing)
- > Or quick fix: use secure DNS to get VPN server's IP address

Disclosure

- > Reported to CERT/CC on May 10, 2023
- > Reported to selected vendors that had a security contact:
 - » Some had no e-mail contact, only a bug bounty program
 - >> In report say we deviate from T&Cs and reserve right to disclose

Disclosure: special cases



Dubai-based ClarioVPN

- > Initially: "MitM attacks are out of scope"
- Later: "Clario isn't interested in participating in this multi-party disclosure on VPN security"



Ivanti Pulse Secure

- > Provided a test server! But at first didn't work
- > Kept asking for time-consuming recordings
- > Seems like they didn't try our PoC script...

Conclusion

- > Two wide-spread flaws in VPN clients
- > In hindsight easy attack, but ~66% vulnerable
- > Bad integration of protocols into real systems

- > Defense: more carefully configure routing tables
 - > OS should have API to create VPN tunnels





Questions?



- > Two wide-spread flaws in VPN clients
- > In hindsight easy attack, but ~66% vulnerable
- > Bad integration of protocols into real systems





- > Defense: more carefully configure routing tables
- > OS should have API to create VPN tunnels