Tunnel Vision Attack
Most VPNs Exposed to Surveillance Risks

TunnelVision is a cybersecurity threat targeting virtual private network (VPN) traffic. This attack exposes VPN traffic to potential snooping or tampering, fundamentally compromising the intended protection provided by VPNs.

Researchers behind TunnelVision have uncovered a flaw affecting nearly all VPN applications. This flaw compels the VPNs to route some or all traffic outside of the encrypted tunnel, which is designed to safeguard data from interception or manipulation.

Named TunnelVision, this attack essentially nullifies the primary purpose of VPNs: to encapsulate both incoming and outgoing internet traffic within an encrypted tunnel, thus obscuring the user's IP address. It affects virtually all VPN applications when they're connected to a hostile network. Global reports let us estimate that this kind of threat has been on the web since 2002 and could have been exploited in the wild.

The impact of TunnelVision is profound. It allows attackers to intercept, drop, or modify the leaked traffic while the victim remains connected to both the VPN and the internet. The attack manipulates the DHCP (Dynamic Host Configuration Protocol) server, which assigns IP addresses to devices connecting to the local network. By exploiting a setting known as option 121, the attacker reroutes VPN traffic through the DHCP server, diverting it away from the intended encrypted tunnel.

This attack can be executed most effectively by individuals with administrative control over the network being targeted. However, even unprivileged users can potentially carry out the attack by setting up a rogue DHCP server. Once successful, the attack exposes some or all traffic to potential interception, undermining the confidentiality and integrity of the VPN connection.

Notably, Android is immune to TunnelVision due to its lack of implementation of option 121. However, for other operating systems, complete fixes are currently unavailable. Although Linux offers a partial mitigation by minimizing the attack's impact, TunnelVision can still exploit a side channel for de-anonymization and targeted denial-of-service attacks.

When we talk about the Internet, one of the most used services everyone is DHCP, but, it has four well-known vulnerabilities:

- **DHCP Spoofing**: This occurs when an attacker impersonates a legitimate DHCP server on the network and assigns IP addresses to clients. By doing so, the attacker can redirect traffic to malicious destinations or intercept sensitive information.
- **DHCP Denial-of-Service (DoS)**: Attackers can flood the DHCP server with an overwhelming number of DHCP requests, causing it to become unresponsive and denying service to legitimate clients. This can disrupt network connectivity and prevent devices from obtaining valid IP addresses.
- **DHCP Relay Agent Vulnerabilities**: DHCP relay agents are used to forward DHCP messages between clients and servers across different network segments. Vulnerabilities in these relay agents can be exploited by attackers to intercept or manipulate DHCP messages, leading to potential network disruptions or security breaches.
- **DHCP Client Vulnerabilities**: Vulnerabilities in DHCP client implementations can be exploited by attackers to execute arbitrary code, escalate privileges, or perform other malicious

activities on the client device. These vulnerabilities may arise due to buffer overflows, input validation errors, or insecure configuration settings.

From today, I suggest adding Tunnel Vision too.

Moreover installing a free or a business VPN still exposes everyone to several risks. Using a VPN everyone still meets these risks:

1. **Logging Policies**: Some VPN providers may keep logs of user activity, including browsing history, connection timestamps, and IP addresses. If these logs are compromised or subpoenaed, it could compromise user privacy and anonymity.
2. **Data Leaks**: VPNs can sometimes suffer from data leaks, where a user's real IP address or DNS requests are inadvertently exposed to third parties due to misconfigurations or vulnerabilities in the VPN software.
3. **Malware Distribution**: Malicious actors may set up fake VPN services or compromise legitimate VPN providers to distribute malware to unsuspecting users. Users may inadvertently download and install malware when using compromised VPN services.
4. **Traffic Interception**: In some cases, attackers may intercept VPN traffic using techniques such as man-in-the-middle (MITM) attacks. This allows them to eavesdrop on sensitive data transmitted over the VPN connection, potentially compromising user privacy and security.
5. **Insecure Protocols**: Some VPN protocols, such as Point-to-Point Tunneling Protocol (PPTP), may be vulnerable to security flaws and encryption weaknesses. Using insecure protocols can expose VPN users to various security risks, including interception and decryption of their data.
6. **VPN Provider Trust**: Users must trust their VPN provider with their data, as all internet traffic passes through the VPN server. If a VPN provider is untrustworthy or compromised, it could result in unauthorized access to user data or surveillance by third parties.
7. **Government Surveillance**: In some jurisdictions, governments may require VPN providers to cooperate with surveillance efforts or disclose user data. This can undermine the privacy and anonymity offered by VPN services, particularly if the VPN provider is compelled to log user activity or share data with authorities.
8. **DNS Leaks**: DNS leaks occur when DNS requests bypass the VPN tunnel and are resolved by the user's ISP's DNS servers. This can expose the websites visited by the user, even when connected to a VPN, potentially compromising privacy.
9. **Limited Security Measures**: Not all VPN providers implement robust security measures, such as strong encryption, secure VPN protocols, or regular security audits. Choosing a reputable VPN provider with strong security practices is essential for mitigating these risks.
10. **Subscription Scams and Fraud**: Users may fall victim to subscription scams or fraudulent VPN services that promise security and anonymity but fail to deliver. These services may collect user data, engage in deceptive practices, or provide inadequate security protections.

VPN users need to be aware of these risks and take proactive steps to mitigate them, such as choosing reputable VPN providers, using strong encryption protocols, and regularly updating VPN software. Additionally, users should be cautious when accessing sensitive information or performing online transactions over VPN connections to minimize the risk of data compromise.

Finally, **effective remedies for Tunnel Vision Attacks include running the VPN inside a virtual machine with a network adapter in non-bridged mode or connecting the VPN through a cellular device's Wi-Fi network**. *These solutions help mitigate the risk posed by TunnelVision, safeguarding VPN traffic from potential interception and manipulation*.

Author: Alessandro Civati.