[Solution Brief]

Understanding TunnelVision - A VPN Evasive Attack

TunnelVision is an emerging cyber threat that targets the security of VPN connections by exploiting the Dynamic Host Configuration Protocol (DHCP). This attack, identified by its vulnerability identifier CVE-2024-3661, is notable for its ability to route VPN traffic outside of its encrypted tunnel, making the traffic visible and manipulable by attackers.

MECHANISM OF THE ATTACK

The core of the TunnelVision attack involves the manipulation of the VPN's routing table through DHCP option 121. This option allows for the configuration of classless static routes directly on a client's system. Attackers establish a rogue DHCP server on the same network as the targeted VPN user and manipulate this server to reroute the victim's traffic through a gateway controlled by the attackers, rather than through the VPN's secure tunnel.

This manipulation is subtle enough that the VPN appears to be functioning normally to the user, maintaining the illusion of a secure, private connection while the traffic is actually being intercepted and potentially altered.

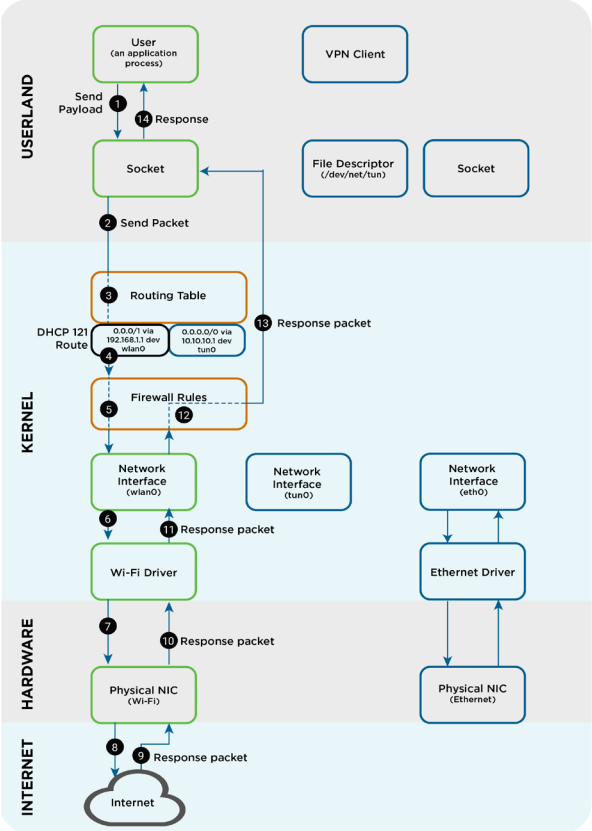
IMPACT AND IMPLICATIONS

The implications of TunnelVision are particularly severe for entities that depend heavily on VPNs for secure and private communication. Given that the attack leverages a common protocol feature, it affects a wide range of operating systems including Windows, macOS, Linux, and iOS, with Android being the exception due to its lack of support for DHCP option 121.

MITIGATION STRATEGIES

To defend against TunnelVision attacks, several mitigation strategies have been proposed:

- **Network Isolation:** Using network namespaces on Linux to isolate network interfaces and prevent rogue DHCP configurations from affecting VPN traffic.
- **Strict Traffic Rules:** Configuring VPN clients to reject all traffic that does not originate from the VPN interface, with exceptions only for necessary communications.
- **Ignoring DHCP Option 121:** This can prevent malicious routing instructions from being applied but might disrupt network connectivity in certain scenarios.
- **Secure Network Practices:** Avoiding the use of untrusted networks, particularly public Wi-Fi, which are ideal environments for such attacks.



EMBRACING ZERO TRUST AND SASE

The discovery of vulnerabilities like TunnelVision underscores the limitations of traditional VPN technologies in today's dynamic cyber environment. This revelation compels a shift towards more robust security frameworks, such as Zero Trust and Secure Access Service Edge (SASE). These models do not inherently trust any entity inside or outside the network, requiring verification at every step of digital interaction, which significantly mitigates the risk of such vulnerabilities.

Zero Trust emphasizes the principle of "never trust, always verify," ensuring that only authenticated and authorized users and devices can access applications and data. This approach effectively counters the risks posed by compromised network segments or rogue DHCP servers, as seen with TunnelVision, because it minimizes the potential impact of attacks that exploit the trust assumptions of traditional network security.

SASE, on the other hand, combines network security functions (such as SWG, CASB, FWaaS, and ZTNA) with WAN capabilities (like SD-WAN) to support the dynamic secure access needs of organizations. By integrating these services through a cloud architecture, SASE provides secure and fast cloud adoption, and a unified point of control to mitigate threats across all locations and users. This holistic approach is especially effective against network-based attacks by ensuring that security policies are uniformly applied, no matter where the users and resources are located.

As cyber threats evolve, adopting a Zero Trust architecture integrated with SASE offers a forward-looking strategy that can adapt to changes in the threat landscape, enhance security postures, and protect critical assets more effectively than conventional VPN solutions.

ABOUT SDG

SDG is a leading provider of technology, consulting, and managed services that enable organizations to confidently execute cloud, cybersecurity, identity, and risk management solutions to mitigate risk, protect assets, and grow securely.

To learn how SDG can help your organization, visit SDGC.com or call us, +1 203.866.8886.

SDG

75 North Water Street
Norwalk, CT 06854

203.866.8886

sdgc.com

Special Article by Soumak Roy
SDG, Vice President – Cybersecurity