CRITICALSTART®

The VPN Man-in-the-Middle: TunnelVision and the Urgent Need for Stronger Security

Organizations and individual users leveraging Virtual Private Networks (VPNs) for secure remote access should be aware of a recently discovered technique called TunnelVision. This technique exploits a vulnerability within the Dynamic Host Configuration Protocol (DHCP) to manipulate routing tables. By doing so, attackers can potentially force VPN traffic outside the encrypted tunnel and redirect it through a server under their control. This effectively bypasses VPN encryption, exposing sensitive data transmitted over the network, such as login credentials or financial information.

TunnelVision poses a multifaceted threat to organizations across various industries. The potential for sensitive data breaches, financial losses, reputational damage, disrupted operations, and even national security risks necessitates a proactive approach to mitigating this vulnerability. Organizations must prioritize robust security measures, including educating employees about cyber hygiene practices, implementing network monitoring tools to detect suspicious activity, and staying updated on the latest security threats like TunnelVision. By taking a proactive stance, organizations can minimize the risk of falling victim to this sophisticated attack technique.

This report contains valuable insights for navigating the evolving cyber landscape. To unlock the full content, reach out to your customer success manager or email info@criticalstart.com.

CRITICALSTART® offers a pioneering solution to modern organizational challenges in aligning cyber protection with risk appetite through its Cyber Operations Risk & Response™ platform, award-winning Managed Detection and Response (MDR) services, and a dedicated human-led risk and security team. By providing continuous monitoring, mitigation, maturity assessments, and comprehensive threat intelligence research, they enable businesses to proactively protect critical assets with measurable ROI. Critical Start's comprehensive approach allows organizations to achieve the highest level of cyber risk reduction for every dollar invested, aligning with their desired levels of risk tolerance.