May 13, 2024

Overall Rating - High

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that TunnelVision hack allows attackers to bypass VPN protections.

Technical Details

DHCP can add routes to a client's routing table via the classless static route option (121). VPN-based security solutions that rely on routes to redirect traffic can be forced to leak traffic over the physical interface. An attacker on the same local network can read, disrupt, or possibly modify network traffic that was expected to be protected by the VPN.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-3661
- New attack leaks VPN traffic using rogue DHCP servers (bleepingcomputer.com)
- TunnelVision hack allows attackers to bypass VPN protections | PCWorld
- CVE-2024-3661: TunnelVision - How Attackers Can Decloak Routing-Based VPNs For a Total VPN Leak — Leviathan Security Group - Penetration Testing, Security Assessment, Risk Advisory