مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

New TunnelVision Attack Exposes VPN Traffic via DHCP Manipulation

Tracking #:432315840

Date:10-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed A recently discovered vulnerability, dubbed TunnelVision, allows attackers to bypass Virtual Private Network (VPN) encryption and steal sensitive information by manipulating a user's routing tables.

TECHNICAL DETAILS:

A recently discovered vulnerability, dubbed TunnelVision (CVE-2024-3661), allows attackers to bypass Virtual Private Network (VPN) encryption and potentially steal or modify your data. This attack leverages manipulation of DHCP (Dynamic Host Configuration Protocol) messages to redirect traffic outside the secure VPN tunnel.

- **CVE-2024-3661**
- CVSS Score: 7.6 HIGH
- TunnelVision, is a vulnerability that affects Virtual Private Networks (VPNs). It allows attackers on the same local network to potentially bypass VPN encryption and snoop on your traffic.
- TunnelVision exploits the fact that DHCP messages lack authentication, allowing attackers to manipulate routing options (specifically, classless static route - Option 121) on a compromised DHCP server.
- By tricking the victim's device into using the attacker's server, the attack redirects VPN traffic outside the encrypted tunnel.
- The attacker can then intercept and potentially alter the traffic before forwarding it to the legitimate gateway.
- This creates a situation where the user remains unaware of the compromised VPN connection, believing their traffic is secure.

Impact

- All operating systems except Android (which doesn't use DHCP option 121) are vulnerable if they support DHCP option 121 routes.
- VPNs relying solely on routing rules for traffic protection are susceptible.
- Attackers can steal confidential information, disrupt ongoing communication, or even modify data in transit.

RECOMMENDATIONS:

- **Avoid untrusted networks:** Whenever possible, avoid using public Wi-Fi or untrusted networks for sensitive activities**.**
- Consider using additional security measures like endpoint firewalls for enhanced protection.
- Implement DHCP snooping on network switches to prevent unauthorized DHCP servers.
- Enable ARP protection to prevent Address Resolution Protocol (ARP) spoofing.
- Enforce port security on switches to restrict unauthorized access.
- Consider using network namespaces on Linux systems for additional protection.
- Ensure operating system, VPN client, and other software are updated with the latest security patches.
- Verify that your VPN provider is aware of and addressing TunnelVision.

- Consider using a reputable VPN service with a strong security track record.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.zscaler.com/blogs/security-research/cve-2024-3661-k-tunnelvision-exposes-vpn-bypass-vulnerability