

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Unveiling The TunnelCrack VPN Vulnerabilities

Date of Publication

August 16, 2023

Admiralty Code

A1













TA Number

TA2023333

Summary

The Tunnelcrack vulnerabilities are a set of four vulnerabilities that affect most VPN products. The vulnerabilities affect the way that VPNs handle certain ciphers, which are algorithms used to encrypt traffic. By exploiting these vulnerabilities, attackers can force the VPN to send traffic outside of the encrypted tunnel, where it can be read by the attacker. Upgrading VPN products as soon as possible is crucial to prevent the exposure of sensitive information to attackers.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-35838	WireGuard Client Denial of Service Vulnerability	WireGuard Client			
CVE-2023-36673	Avira Phantom VPN DNS Spoofing Vulnerability	Avira Phantom VPN			
CVE-2023-36672	Clario VPN Plaintext Traffic Leakage Vulnerability	Clario VPN			
CVE-2023-36671	Clario VPN Traffic to The Real IP Address of The VPN Server Vulnerability	Clario VPN			

Vulnerability Details

#1

The recent exposure of the TunnelCrack VPN vulnerabilities has brought attention to potential security issues almost in all VPN services. These vulnerabilities pertain to the attack itself rather than being specific to particular products. These vulnerabilities specifically focus on the LocalNet and ServerIP attack vectors. Both attacks are claimed to be impacting VPNs for iPhones, iPads, MacBooks, and macOS, a majority of VPNs on Windows and Linux, and roughly one-quarter VPN apps in Android.

#2

In the LocalNet attack, vulnerabilities are identified on specific platforms, with a focus on iOS. The attack leverages the exposure of network traffic outside the VPN tunnel due to local network sharing settings. This could result in a denial of service (DoS) scenario and possible traffic leakage, though the practical impact is debated.

#3

The ServerIP attack vector involves tricking VPN clients into using malicious IP addresses or leaking traffic to the VPN server IP outside the tunnel. This exploit relies on weak firewall configurations and the misuse of DNS to obtain server IPs. Notably, certain VPN clients are found to be vulnerable to this attack due to their routing and firewall rules. This can potentially lead to data exposure and compromise of user privacy.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-35838	WireGuard Client 0.5.3 on Windows	cpe:2.3:a:wireguard:client:0.5.3:*	CWE-200
CVE-2023-36673	Avira Phantom VPN through 2.23.1 for macOS	cpe:2.3:a:avira:phantom_vpn:*	CWE-200
CVE-2023-36672	Clario VPN client through 5.9.1.1662 for macOS	cpe:2.3:a:clario:vpn_client:*	CWE-200
CVE-2023-36671	Clario VPN client through 5.9.1.1662 for macOS	cpe:2.3:a:clario:vpn_client:*	CWE-200

Recommendations



Update VPN Software: Keep your VPN software up to date by installing the latest vendor-provided updates. Regular updates often include critical security patches that address vulnerabilities, reducing the risk of exploitation.



Disable Local Network Sharing (if applicable): If your VPN application features a local network sharing option, consider disabling it. This step can help mitigate the LocalNet attack vector, minimizing the potential for traffic leaks on vulnerable platforms.



Enhance Firewall Rules and DNS Security: VPN providers should strengthen firewall rules to allow outgoing traffic only to the VPN server's IP, port, and protocol. Additionally, prioritize secure DNS resolution through protocols like DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) to prevent DNS-based attacks.

Potential MITRE ATT&CK TTPs

<u>TA0003</u> Persistence	<u>TA0040</u> Impact	<u>TA0006</u> Credential Access	<u>TA0005</u> Defense Evasion
<u>TA0001</u> Initial Access	<u>T1498</u> Network Denial of Service	<u>T1562</u> Impair Defenses	<u>T1562.006</u> Indicator Blocking
<u>T1040</u> Network Sniffing			

🔗 Patch Details

As of now, patches for these vulnerabilities have not been released. Check with Vendor for availability of patches and apply patches as soon as it is available.

🔗 References

<https://tunnelcrack.mathyvanhoef.com/details.html>

<https://mullvad.net/de/blog/2023/8/9/response-to-tunnelcrack-vulnerability-disclosure/>

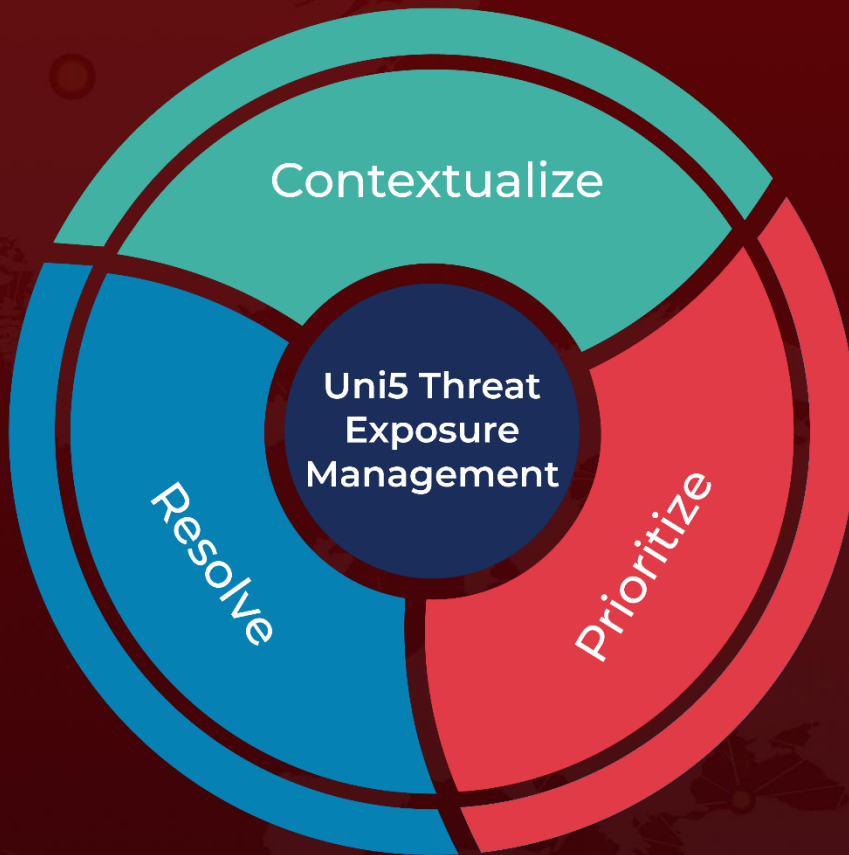
<https://www.helpnetsecurity.com/2023/08/14/vpn-vulnerabilities-tunnelcrack-attacks/>

<https://www.cisa.gov/news-events/bulletins/sb23-226>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

August 16, 2023 • 8:00 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com