(https://cyberinsider.com/)

GrapheneOS fixes Android VPN leak Google refused to patch

May 6, 2026 *By* Alex Lekander (https://cyberinsider.com/author/alexlekander/) —

GrapheneOS has released a new update that fixes a recently disclosed Android VPN bypass vulnerability capable of leaking a user's real IP address.

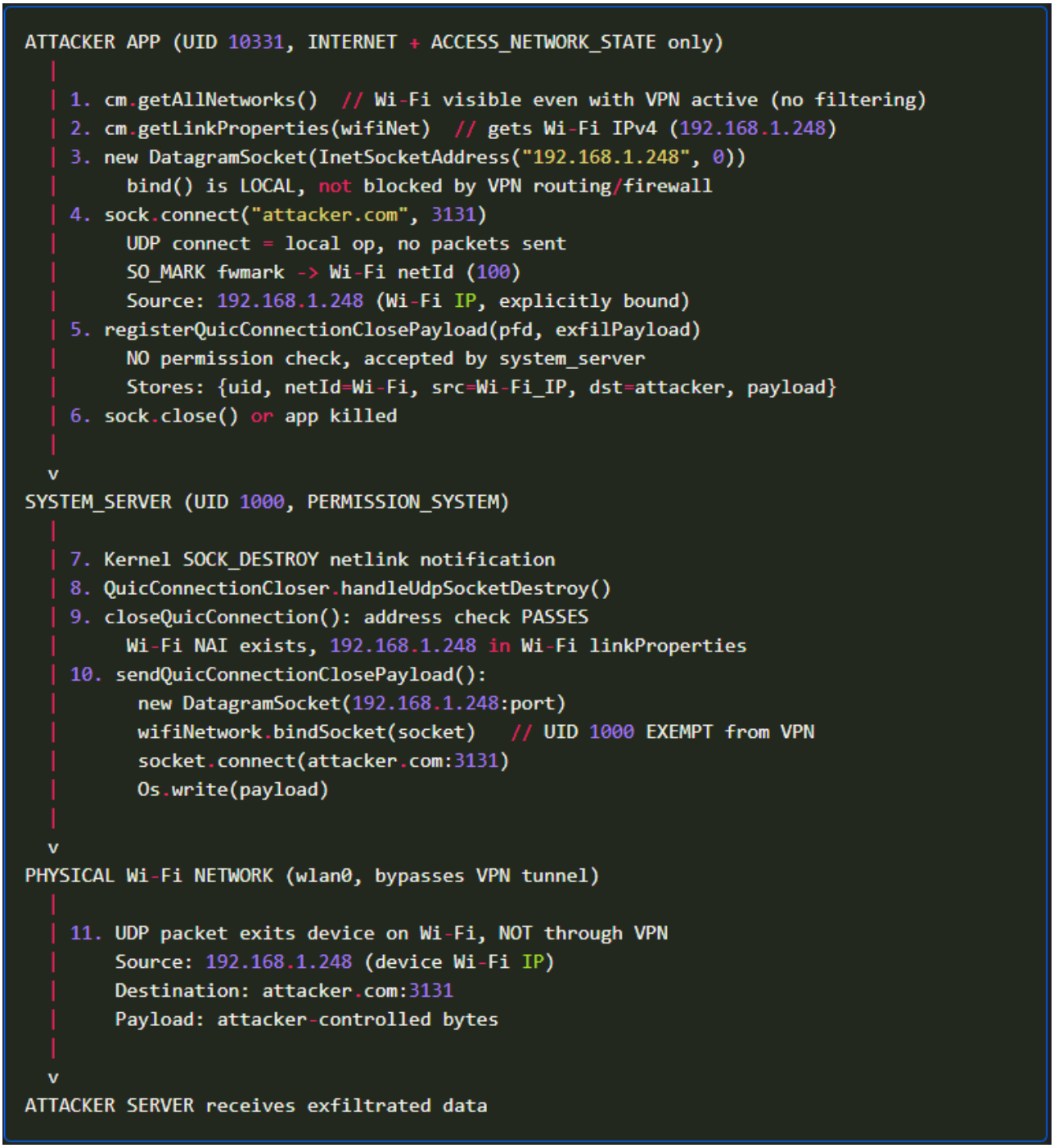
The leak happens even when Android's "Always-On VPN" and "Block connections without VPN" protections were enabled.

The issue, disclosed last week by security researcher "lowlevel/Yusuf," affected Android 16 and stemmed from a newly introduced QUIC connection teardown feature in Android's networking stack. In its latest release, GrapheneOS says it has "disable[d] registerQuicConnectionClosePayload optimization to fix VPN leak," effectively neutralizing the attack vector on supported Pixel devices.

GrapheneOS is a privacy- and security-focused Android-based operating system primarily developed for Google Pixel devices. The project is widely used by privacy-conscious consumers, journalists, activists, and enterprise users seeking stronger application sandboxing, exploit mitigations, and reduced reliance on Google services.

According to Yusuf's technical write-up (https://lowlevel.fun/posts/tiny-udp-cannon-android-vpn-bypass/), the vulnerable API allowed ordinary applications with only the automatically granted INTERNET and ACCESS_NETWORK_STATE permissions to register arbitrary UDP payloads with system_server.

When the app's UDP socket was later destroyed, Android's privileged system_server process would transmit the stored payload directly over the device's physical network interface rather than through the VPN tunnel. Because system_server operates with elevated networking privileges and is exempt from VPN routing restrictions, the packet bypassed Android's VPN lockdown protections entirely.



Attack flow overview

lowlevel.fun

The researcher demonstrated the flaw on a Pixel 8 running Android 16 with Proton VPN enabled alongside Android's lockdown mode. The app reportedly leaked the device's actual public IP address to a remote server despite VPN protection being fully enabled.

Google introduced a feature that allows applications to gracefully terminate QUIC sessions when sockets are unexpectedly destroyed. However, the implementation accepted arbitrary payloads without validating whether they were legitimate QUIC CONNECTION_CLOSE frames and did not verify whether the originating application was restricted to VPN-only traffic.

The researcher reported the issue to Android's security team, which classified it as "Won't Fix (Infeasible)" and "NSBC" (Not Security Bulletin Class), stating that it did not meet the threshold for inclusion in Android security advisories. The researcher appealed the decision, arguing that any application could leak identifying network information using only standard permissions, but Google maintained its position, authorizing public disclosure on April 29.

GrapheneOS responded by disabling the underlying optimization entirely in release 2026050400 (https://grapheneos.org/releases#2026050400).

> *kudos to @GrapheneOS (https://twitter.com/GrapheneOS?ref_src=twsrc%5Etfw) for shipping a fix in less than a weekhttps://t.co/lF7pNCETQ4 (https://t.co/lF7pNCETQ4) https://t.co/otKgCBSKl3 (https://t.co/otKgCBSKl3)*
>
> *— Yusuf (@cybaqkebm) May 5, 2026 (https://twitter.com/cybaqkebm/status/2051724305247989841?ref_src=twsrc%5Etfw)*

Beyond the VPN leak fix, the latest release also includes the full May 2026 Android security patch level, multiple hardened_malloc improvements, Linux kernel updates across Android's 6.1, 6.6, and 6.12 branches, and a backported fix for CVE-2026-33636 in libpng. The update additionally ships newer Vanadium browser builds and expanded Dynamic Code Loading restrictions.

The researcher noted that stock Android users could temporarily mitigate the issue manually through ADB by disabling the close_quic_connection DeviceConfig flag. However, that workaround requires developer access and may not persist indefinitely if Google removes the feature flag in future updates.

If you liked this article, be sure to follow us on **X/Twitter (https://twitter.com/CyberInsidercom)** and also **LinkedIn (https://www.linkedin.com/company/cyberinsider/)** for more exclusive content.

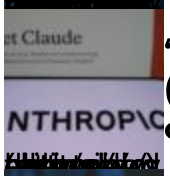
More from CyberInsider

Apple and Meta warn Canada's Bill C-22 forces encryption backdoors (https://cyberinsider.com/apple-and-meta-warn-canadas-bill-c-22-forces-encryption-backdoors/)

EU calls VPNs "a loophole that needs closing" in age verification push (https://cyberinsider.com/eu-calls-vpns-a-loophole-that-needs-closing-in-age-verification-push/)

Former IT contractor convicted for wiping 96 US government databases (https://cyberinsider.com/former-it-contractor-convicted-for-wiping-96-us-government-databases/)

Canvas outage hits thousands of universities as ShinyHunters threatens leak (https://cyberinsider.com/canvas-outage-hits-thousands-of-universities-as-shinyhunters-threatens-leak/)



"ClaudeBleed" allows any Chrome extension to control Anthropic's AI assistant (https://cyberinsider.com/claudebleed-allows-any-chrome-extension-to-control-anthropics-ai-assistant/)

New TCLBANKER malware self-spreads through WhatsApp and Outlook (https://cyberinsider.com/new-tclbanker-malware-self-spreads-through-whatsapp-and-outlook/)

About Alex Lekander

Alex Lekander is the Editor-in-Chief and owner of CyberInsider.com. With a passion for cybersecurity and privacy topics, Alex launched this website in 2020. His background and expertise cover privacy research, technical writing, software testing, and site administration. He holds a Bachelor of Science and a Master of Science from Johns Hopkins University.