PureVPN no Linux: pesquisador encontra problemas de segurança e anon

Data: 2025-09-22 19:13:10

Autor: Inteligência Against Invaders

Redazione RHC**:22 Setembro 2025 21:12**

Um pesquisador independente chamado Andreas, que dirige o blog **Anagogistis** , descobriu vulnerabilidades graves em **Clientes Linux da Pure VPN** esse compromisso *anonimato básico e segurança de tráfego.* Os problemas afetam tanto o *versões gráficas (2.10.0) e de console (2.0.1). Ambos foram testados no Ubuntu 24.04.3 LTS.*

A principal vulnerabilidade surge porque, ao se reconectar ao Wi-Fi ou acordar o sistema do modo de suspensão, **o verdadeiro endereço IPv6 do usuário se torna visível.** No cliente de console com o recurso Internet Kill Switch ativado, o serviço relata automaticamente a retomada da conexão, mas durante esse tempo o sistema recebe rotas IPv6 via Anúncio de Roteador, **fazendo com que os pacotes ignorem o túnel VPN.** Como a política ip6tables permanece ACCEPT por padrão, o tráfego sai do computador diretamente.

O cliente gráfico apresenta um risco ainda maior. Quando a conexão é interrompida, ele bloqueia corretamente o IPv4 e exibe uma notificação de perda de sessão, mas o tráfego IPv6 continua a fluir sem restrições até que o usuário clique manualmente no botão Reconectar. **Isso deixa um atraso significativo durante o qual os dados são transmitidos para a Internet aberta.**

Igualmente perigoso é o *Tratamento de firewall pelo cliente* Configurações. Ao estabelecer uma conexão VPN, ele apaga completamente a configuração existente do iptables, define INPUT como ACCEPT e exclui regras personalizadas, incluindo *UFW, Cadeia do Docker* e suas próprias políticas de segurança. Depois que a conexão VPN for encerrada, *Essas alterações não são revertidas, deixando o sistema mais vulnerável do que antes da conexão.*

O especialista que identificou os problemas *enviou relatórios detalhados e vídeos de demonstração para a PureVPN por meio do programa de divulgação de vulnerabilidades da empresa no final de agosto de 2025.* No entanto, por três semanas, o serviço não respondeu ou forneceu aos usuários informações sobre os riscos.

Na prática, isso significa que *Os usuários do cliente PureVPN Linux podem acessar sites habilitados para IPv6 ou enviar e-mails com a confiança de que a VPN está funcionando, mesmo que seu endereço real já tenha sido divulgado ao provedor* . A presença simultânea de uma falha IPv6 e regras de firewall corrompidas indica uma violação fundamental dos princípios fundamentais de segurança nos quais se baseia a confiança nos serviços VPN.

Redação
A equipe editorial da Red Hot Cyber é composta por um grupo de indivíduos e fontes anônimas que colaboram ativamente para fornecer informações e notícias antecipadas sobre segurança cibernética e computação em geral.

Lista degli articoli