BOLETIM DE SEGURANÇA

Vulnerabilidade TunnelVision realiza captura de dados em redes VPN através de técnicas de DHCP

heimdall
security research
A DIVISION OF ISH

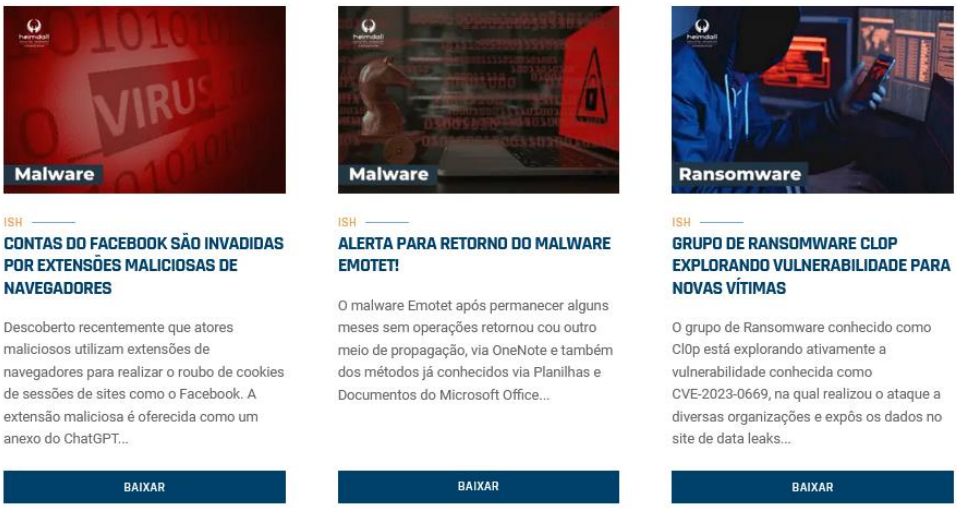
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

1 SUMÁRIO EXECUTIVO

Especialistas revelaram um método conhecido como TunnelVision, que é uma vulnerabilidade CVE-2024-3661 classificada como alta em redes privadas virtuais (VPN). Essa falha permite que invasores, ao compartilharem a mesma rede local que a vítima, consigam monitorar e interceptar dados transmitidos, comprometendo a privacidade e segurança das informações.

2 INFORMAÇÕES SOBRE A AMEAÇA

A vulnerabilidade CVE-2024-3661, refere-se de VPNs que estão sendo promovidas como ferramentas de segurança para proteção em redes inseguras, como Wi-Fi público. Contudo, a eficácia dessas ferramentas é debatida no meio de segurança, com relatos de vulnerabilidades. Pesquisas geralmente focam em servidores VPN, mas recentemente, técnicas como TunnelCrack e TunnelVision têm demonstrado riscos de vazamento de dados em redes locais. O TunnelVision, em particular, revelou que invasores na mesma rede podem acessar todo o tráfego de um usuário VPN, apesar da aparente segurança oferecida pela conexão VPN.

Computadores conectados simultaneamente a múltiplas redes utilizam "tabelas de roteamento" para direcionar o tráfego. Invasores na mesma rede podem alterar essas tabelas, redirecionando o tráfego VPN para a rede local, o que compromete a segurança da VPN. A técnica TunnelVision explora essa vulnerabilidade sem necessitar de acesso ao servidor DHCP, funcionando independentemente do tipo de VPN utilizada. Os usuários que recorrem a VPNs para segurança em redes duvidosas não estão imunes aos ataques típicos dessas redes, mesmo com o uso de VPNs. Isso representa um risco elevado para usuários que dependem dessa tecnologia para proteção, incluindo jornalistas e opositores políticos. A falsa sensação de segurança pode ser tão perigosa quanto a ausência de proteção.

A boa notícia é que a maior parte do tráfego de internet dos usuários de VPNs comerciais é criptografado via HTTPS, representando aproximadamente 85% do total. Embora essa criptografia torne os dados ininteligíveis para possíveis interceptadores utilizando ferramentas como o Tunnelvision, a identidade do destinatário do tráfego ainda é visível, o que pode representar uma vulnerabilidade. No caso de sites que utilizam HTTP, não só o destinatário como também o conteúdo da comunicação fica exposto aos olhares alheios. Nas pesquisas recentes colocam em xeque o entendimento que se tinha sobre as VPNs. Além disso, suscitam dúvidas acerca de outras tecnologias que podem ser comprometidas por ataques às tabelas de roteamento, um problema que parece ter permanecido oculto por mais de duas décadas.

3 RECOMENDAÇÕES

DHCP Snooping

- Ativar o DHCP snooping em switches de LAN pode ajudar a prevenir servidores DHCP fraudulentos, eliminando tráfego DHCP potencialmente nocivo. Esta medida garante acesso à rede apenas para clientes com endereços IP e/ou MAC especificados e oferece segurança adicional para pacotes ARP.

Segurança de porta

- Configurar a segurança de porta em switches de rede para limitar o número de endereços MAC aprendidos por porta. Isso garante que o switch encaminhe apenas pacotes com endereços MAC reconhecidos, bloqueando eficazmente pacotes falsos.

Ignorar a opção 121 do DHCP

- Quando o VPN está ativo na rede, pode ser benéfico ignorar a opção 121 do DHCP, que adiciona rotas estáticas sem classe à tabela de roteamento do cliente. No entanto, é importante notar que ignorar esta opção pode causar problemas de conectividade de rede em alguns cenários.

Espaços de nomes de rede para provedores de VPN

- Recomenda-se que os provedores de VPN integrem espaços de nomes de rede nos sistemas operacionais suportados para isolar interfaces e tabelas de roteamento do controle da rede local, aumentando assim a segurança contra ataques que exploram essa vulnerabilidade.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Tunnelvisionbug
- Thehackernews
- NVD

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH