Una nueva investigación ha identificado vulnerabilidades de seguridad en varios protocolos de túnel que podrían ser explotadas por atacantes para realizar diversas acciones maliciosas.

> *«Los hosts de Internet que aceptan paquetes de túnel sin confirmar la identidad del remitente pueden ser utilizados para llevar a cabo ataques anónimos y acceder a sus redes internas»*, indicó Top10VPN en un informe elaborado en colaboración con Mathy Vanhoef, profesor e investigador de la universidad KU Leuven.

Se estima que unos 4,2 millones de dispositivos, incluidos servidores VPN, routers domésticos de proveedores de servicios de Internet (ISP), routers centrales, gateways de redes móviles y nodos de redes de distribución de contenido (CDN), son vulnerables a estas amenazas. Los países más afectados son China, Francia, Japón, Estados Unidos y Brasil.

La explotación exitosa de estas fallas permite a los atacantes utilizar los sistemas comprometidos como proxies unidireccionales o para realizar ataques de denegación de servicio (DoS).

> *«Un atacante puede aprovechar estas vulnerabilidades para crear proxies unidireccionales y falsificar direcciones IPv4/6 de origen. Además, los sistemas afectados pueden ser utilizados para acceder a redes privadas corporativas o ejecutar ataques DDoS»,* advirtió el CERT Coordination Center (CERT/CC) en una notificación.

Estas vulnerabilidades surgen porque protocolos de túnel como IP6IP6, GRE6, 4in6 y 6in4, diseñados para transferir datos entre redes desconectadas, no incluyen mecanismos de autenticación ni cifrado sin la implementación de medidas de seguridad adicionales, como IPsec.

La falta de protecciones de seguridad adicionales deja abierta la posibilidad de que un

atacante inyecte tráfico malicioso en los túneles. Esto es similar a un fallo previamente identificado en 2020 (CVE-2020-10136).

Los siguientes identificadores CVE han sido asignados a estas vulnerabilidades:

- CVE-2024-7595 (GRE y GRE6)
- CVE-2024-7596 (Encapsulación Genérica UDP)
- CVE-2025-23018 (IPv4-in-IPv6 y IPv6-in-IPv6)
- CVE-2025-23019 (IPv6-in-IPv4)

> *«El ataque consiste en enviar un paquete encapsulado con uno de los protocolos vulnerables que contiene dos encabezados IP»,* explicó Simon Migliano de Top10VPN.
>
> *«El encabezado externo lleva la dirección IP del atacante como origen y la del host vulnerable como destino. Por otro lado, el encabezado interno simula que la dirección IP de origen es la del host vulnerable, mientras que la dirección de destino apunta al objetivo del ataque».*

Cuando el host vulnerable recibe el paquete, elimina el encabezado IP externo y reenvía el paquete interno a su destino. Dado que el encabezado interno tiene la IP del host vulnerable, que es confiable, el tráfico pasa sin ser bloqueado por los filtros de red.

Para mitigar estos riesgos, se recomienda utilizar protocolos como IPSec o WireGuard para garantizar la autenticación y el cifrado, y aceptar únicamente paquetes de túnel provenientes de fuentes confiables. Además, a nivel de red, es aconsejable implementar filtros de tráfico en routers y dispositivos intermedios, realizar inspecciones profundas de paquetes (DPI) y bloquear todos los paquetes de túnel sin cifrar.

> *«Las víctimas de estos ataques DoS pueden experimentar congestión de red, interrupción de servicios debido al consumo excesivo de recursos, e incluso el colapso de dispositivos de red sobrecargados. Estas brechas también podrían ser aprovechadas para otros tipos de ataques, como interceptación de datos o ataques de intermediario (man-in-the-middle)»,* advirtió Migliano.