Se han identificado dos fallos de seguridad en la suite de herramientas de red segura OpenSSH que, si son explotados con éxito, podrían derivar en un ataque activo de intermediario (MitM) y en una denegación de servicio (DoS), respectivamente, bajo ciertas circunstancias.

Las vulnerabilidades, documentadas por el equipo de investigación de amenazas de Qualys (TRU), son las siguientes:

- CVE-2025-26465: El cliente de OpenSSH presenta un error lógico en las versiones comprendidas entre la 6.8p1 y la 9.9p1 (ambas incluidas), lo que lo hace susceptible a un ataque MitM si la opción `VerifyHostKeyDNS` está activada. Esto permitiría que un atacante suplante un servidor legítimo cuando un cliente intenta establecer una conexión. (Introducido en diciembre de 2014).
- CVE-2025-26466: Tanto el cliente como el servidor de OpenSSH pueden ser objeto de un ataque DoS antes de la autenticación en las versiones 9.5p1 a 9.9p1 (inclusive), lo que podría causar un consumo elevado de memoria y uso excesivo del procesador. (Introducido en agosto de 2023).

> *«Si un atacante logra llevar a cabo un ataque de intermediario a través de CVE-2025-26465, el cliente podría aceptar la clave del atacante en lugar de la del servidor legítimo»,* explicó Saeed Abbasi, gerente de producto en Qualys TRU.
>
> *«Esto comprometería la seguridad de la conexión SSH, permitiendo la posible interceptación o manipulación de la sesión sin que el usuario lo detecte.»*

En términos prácticos, una explotación exitosa podría permitir que ciberdelincuentes secuestren sesiones SSH y accedan sin autorización a información sensible. Es importante mencionar que la opción `VerifyHostKeyDNS` está desactivada por defecto.

Por otro lado, si CVE-2025-26466 es explotado repetidamente, podría generar problemas de

disponibilidad en los servidores, impidiendo a los administradores gestionarlos y bloqueando el acceso a usuarios legítimos, lo que afectaría el funcionamiento normal de los sistemas.

Ambas vulnerabilidades han sido corregidas en la versión OpenSSH 9.9p2, publicada hoy por los responsables de su mantenimiento.

Este anuncio llega más de siete meses después de que Qualys revelara otra vulnerabilidad en OpenSSH, denominada regreSSHion (CVE-2024-6387), que podría haber permitido la ejecución remota de código sin autenticación con privilegios de administrador en sistemas Linux basados en glibc.