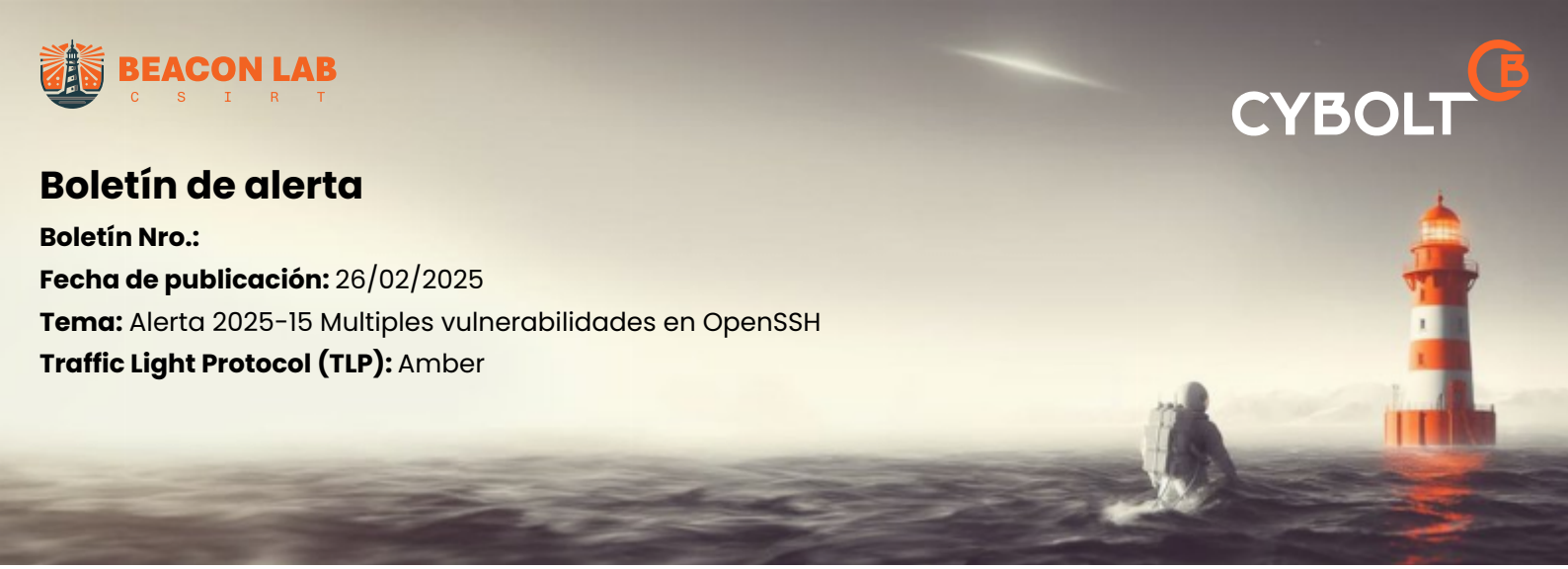

Boletín de alerta

Boletín Nro.:
Fecha de publicación: 26/02/2025
Tema: Alerta 2025-15 Multiples vulnerabilidades en OpenSSH
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

Las vulnerabilidades afectan a diversas versiones de OpenSSH dependiendo de la versión de Linux donde se encuentren ejecutando.

Descripción

Se ha publicado recientemente dos vulnerabilidades que afectan a la herramienta muy conocida y utilizada llamada OpenSSH, estas fallas, identificadas como CVE-2025-26465 (con CVSSv3 6.8) y CVE-2025-26466 (con CVSSv3 5.6), podrían permitir a los atacantes ejecutar ataques de tipo máquina en el medio (MITM) y ataques de denegación de servicio (DoS), respectivamente.

OpenSSH (Open Secure Shell) es un conjunto de herramientas de conectividad de red de código abierto que implementa el protocolo SSH (Secure Shell) para proporcionar comunicaciones seguras a través de redes no confiables. Desarrollado como parte del proyecto OpenBSD, OpenSSH incluye un servidor SSH, un cliente SSH y utilidades relacionadas, como scp y sftp, que permiten la transferencia segura de archivos y la administración remota de sistemas. Es ampliamente utilizado debido a su enfoque en la seguridad, su compatibilidad multiplataforma y su capacidad para reemplazar herramientas menos seguras, como Telnet y FTP, al cifrar todo el tráfico para prevenir ataques como la intercepción de datos o el secuestro de sesiones.

A continuación se describen las vulnerabilidades:

- CVE-2025-26466: Se encontró una falla en el paquete OpenSSH. Por cada paquete ping que recibe el servidor SSH, se asigna un paquete pong en un búfer de memoria y se almacena en una cola de paquetes. Sólo se libera cuando finaliza el intercambio de claves servidor/cliente. Un cliente malintencionado puede seguir enviando dichos paquetes, lo que provoca un aumento incontrolado del consumo de memoria en el lado del servidor. En consecuencia, el servidor puede dejar de estar disponible, lo que resultará en un ataque de denegación de servicio.

- CVE-2025-26465: Se encontró una vulnerabilidad en OpenSSH cuando la opción VerifyHostKeyDNS está habilitada. Un ataque de máquina en el medio puede realizarse mediante una máquina

maliciosa que se haga pasar por un servidor legítimo. Este problema se produce debido a cómo OpenSSH maneja mal los códigos de error en condiciones específicas al verificar la clave del host. Para que un ataque se considere exitoso, el atacante debe lograr agotar primero los recursos de memoria del cliente, lo que aumenta la complejidad del ataque.

Mitigación

- CVE-2025-26466: Este problema se puede mitigar configurando las siguientes tres opciones diferentes en el archivo de configuración sshd ubicado en: /etc/ssh/sshd_config
- MaxStartups: configurada en un valor razonable, esta opción controla la cantidad máxima de conexiones simultáneas no autenticadas que acepta el servidor SSH.
    - PerSourcePenalties: establezca sus subopciones en un valor razonable; esta opción se utiliza para ayudar a sshd a detectar y descartar conexiones que son potencialmente maliciosas para el servidor SSH.
    - LoginGraceTime: configurada en un valor razonable, esta opción controla cuánto tiempo esperará el servidor SSH al cliente para autenticarse antes de interrumpir su conexión.
- CVE-2025-26465: Se recomienda:
- Revisar la configuración: asegúrese de que la opción VerifyHostKeyDNS esté desactivada para evitar posibles ataques MitM.
    - Monitorear sistemas: verifique periódicamente si hay intentos de acceso no autorizados y comportamientos inusuales del sistema.
- Para protegerse de ataques de fuerza bruta, puede utilizar la herramienta Fail2ban.

Solución

Para solucionar ambas vulnerabilidades, CVE-2025-26465 y CVE-2025-26466 se recomienda actualizar a el OpenSSH a la versión 9.9p2.

https://cdn.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-9.9p2.tar.gz

Para mas información sobre la actualización puede dirigirse al siguiente enlace:
https://www.openssh.com/releasenotes.html#9.9p2

Información adicional:

- **OpenSSH Flaws CVE-2025-26465 & CVE-2025-26466 Expose Clients and Servers to Attacks**
- **https://access.redhat.com/security/cve/CVE-2025-26465**
- **https://ubuntu.com/security/CVE-2025-26466**