Los responsables de OpenSSH han lanzado actualizaciones de seguridad para corregir una vulnerabilidad crítica que podría permitir la ejecución remota de código sin autenticación con privilegios de root en sistemas Linux basados en glibc.

La vulnerabilidad, llamada regreSSHion, ha sido identificada con el código CVE-2024-6387. Se encuentra en el componente del servidor OpenSSH, conocido como sshd, que está diseñado para recibir conexiones de cualquier aplicación cliente.

> *«La vulnerabilidad, que es una condición de carrera en el manejador de señales del servidor de OpenSSH (sshd), permite la ejecución remota de código (RCE) sin autenticación como root en sistemas Linux basados en glibc,»* explicó Bharat Jogi, director senior de la unidad de investigación de amenazas en Qualys, en una divulgación publicada hoy. *«Esta condición de carrera afecta a sshd en su configuración predeterminada.»*

La firma de ciberseguridad informó que identificó al menos 14 millones de instancias potencialmente vulnerables del servidor OpenSSH expuestas a Internet, agregando que es una regresión de una falla parcheada hace 18 años, rastreada como CVE-2006-5051, que fue reintroducida en octubre de 2020 como parte de la versión 8.5p1 de OpenSSH.

> *«Se ha demostrado la explotación exitosa en sistemas Linux/glibc de 32 bits con [randomización del diseño del espacio de direcciones]. En condiciones de laboratorio, el ataque requiere en promedio de 6 a 8 horas de conexiones continuas hasta alcanzar el máximo que el servidor aceptará»*, señaló OpenSSH en un aviso.

La vulnerabilidad afecta a las versiones entre 8.5p1 y 9.7p1. Las versiones anteriores a 4.4p1 también son vulnerables al error de condición de carrera a menos que estén parcheadas para CVE-2006-5051 y CVE-2008-4109. Es importante destacar que los sistemas OpenBSD no se ven afectados ya que cuentan con un mecanismo de seguridad que bloquea la falla.

Es probable que la vulnerabilidad también afecte tanto a macOS como a Windows, aunque aún no se ha confirmado su explotabilidad en estas plataformas y se requiere más análisis.

Qualys descubrió que si un cliente no se autentica dentro de los 120 segundos (una configuración definida por LoginGraceTime), entonces el manejador SIGALRM de sshd se llama de manera asincrónica de una forma que no es async-signal-safe.

El efecto neto de explotar CVE-2024-6387 es un compromiso completo del sistema, permitiendo a los atacantes ejecutar código arbitrario con los más altos privilegios, subvertir mecanismos de seguridad, robar datos e incluso mantener acceso persistente.

> *«Una falla, una vez corregida, ha reaparecido en una versión posterior del software, generalmente debido a cambios o actualizaciones que reintroducen inadvertidamente el problema. Este incidente resalta la importancia de realizar pruebas de regresión exhaustivas para evitar la reintroducción de vulnerabilidades conocidas»,* dijo Jogi.

Aunque la vulnerabilidad presenta obstáculos significativos debido a su naturaleza de condición de carrera remota, se recomienda a los usuarios aplicar los últimos parches para protegerse contra posibles amenazas. También se aconseja limitar el acceso SSH a través de controles basados en la red y aplicar segmentación de red para restringir el acceso no autorizado y el movimiento lateral.