Las versiones específicas de la suite de red segura OpenSSH están expuestas a una nueva vulnerabilidad que puede causar la ejecución remota de código (RCE).

La vulnerabilidad, identificada como CVE-2024-6409 (puntuación CVSS: 7.0), es diferente de CVE-2024-6387 (también conocida como RegreSSHion) y se refiere a un caso de ejecución de código en el proceso hijo privsep debido a una condición de carrera en el manejo de señales. Afecta únicamente a las versiones 8.7p1 y 8.8p1 distribuidas con Red Hat Enterprise Linux 9.

El investigador de seguridad Alexander Peslyak, conocido como Solar Designer, ha sido acreditado con el descubrimiento y la denuncia del fallo, que fue encontrado durante una revisión de CVE-2024-6387 después de que este último fuera divulgado por Qualys a principios de este mes.

> *«La principal diferencia con CVE-2024-6387 es que la condición de carrera y el potencial de RCE se activan en el proceso hijo privsep, que se ejecuta con privilegios reducidos en comparación con el proceso padre del servidor»*, explicó Peslyak.
>
> *«Por lo tanto, el impacto inmediato es menor. Sin embargo, pueden existir diferencias en la explotabilidad de estas vulnerabilidades en un escenario particular, lo que podría hacer que una de ellas sea una opción más atractiva para un atacante, y si solo una de estas se corrige o mitiga, entonces la otra se vuelve más relevante».*

Sin embargo, cabe destacar que la vulnerabilidad de la condición de carrera del manejador de señales es la misma que CVE-2024-6387, en la que si un cliente no se autentica dentro del tiempo LoginGraceTime (120 segundos por defecto), entonces el manejador SIGALRM del proceso del demonio OpenSSH se llama de manera asincrónica, lo que luego invoca varias funciones que no son seguras para señales asíncronas.

> *«Este problema lo deja vulnerable a una condición de carrera del manejador de señales en la función cleanup_exit(), que introduce la misma vulnerabilidad que CVE-2024-6387 en el proceso hijo no privilegiado del servidor SSHD»,* según la descripción de la vulnerabilidad.
>
> *«Como resultado de un ataque exitoso, en el peor de los casos, el atacante podría llevar a cabo una ejecución remota de código (RCE) dentro del usuario no privilegiado que ejecuta el servidor sshd».*

Desde entonces, se ha detectado en la naturaleza un exploit activo para CVE-2024-6387, con un actor de amenazas desconocido que ataca principalmente a servidores ubicados en China.

> *«El vector inicial de este ataque proviene de la dirección IP 108.174.58[.]28, la cual se informó que aloja una lista de directorios con herramientas de explotación y scripts para automatizar la explotación de servidores SSH vulnerables»*, indicó la empresa israelí de ciberseguridad Veriti.