Investigadores en ciberseguridad han revelado dos vulnerabilidades en la herramienta de línea de comandos Sudo, utilizada en sistemas Linux y otros sistemas operativos similares a Unix, que podrían permitir a atacantes locales escalar privilegios y obtener acceso como root en sistemas vulnerables.

A continuación se describen brevemente las fallas encontradas:

- CVE-2025-32462 (puntuación CVSS: 2.8) – Las versiones de Sudo anteriores a la 1.9.17p1, cuando se utilizan con un archivo sudoers que incluye un host que no es ni el sistema actual ni «ALL», permiten que los usuarios autorizados ejecuten comandos en máquinas distintas a las esperadas.
- CVE-2025-32463 (puntuación CVSS: 9.3) – En versiones anteriores a Sudo 1.9.17p1, usuarios locales pueden obtener acceso como root porque el archivo «/etc/nsswitch.conf» puede ser tomado desde un directorio controlado por el usuario cuando se utiliza la opción –chroot.

Sudo es una utilidad de consola que permite a usuarios con bajos privilegios ejecutar comandos como si fueran otro usuario, comúnmente el superusuario. Su objetivo es aplicar el principio de mínimo privilegio, es decir, permitir que se realicen tareas administrativas sin necesidad de acceso completo.

La configuración del comando se gestiona mediante el archivo «/etc/sudoers», el cual especifica *"quién puede ejecutar qué comandos como qué usuarios, en qué máquinas, y también puede controlar aspectos especiales como si se requiere contraseña para ciertos comandos".*

El investigador Rich Mirch, de Stratascale, quien descubrió y reportó ambas vulnerabilidades, explicó que CVE-2025-32462 había pasado desapercibida por más de 12 años. Esta falla está relacionada con la opción -h (host) de Sudo, que permite consultar los privilegios de sudo para un host diferente. Esta funcionalidad fue incorporada en septiembre de 2013.

No obstante, debido a un error, era posible ejecutar comandos permitidos para un host

remoto en la máquina local, si se usaba Sudo con la opción host apuntando a un sistema ajeno.

> *"Esto afecta principalmente a entornos que comparten un archivo sudoers común entre múltiples sistemas. Los entornos que utilizan sudoers basados en LDAP (como SSSD) también se ven afectados»,* explicó el responsable del proyecto Sudo, Todd C. Miller, en un comunicado.

En cuanto a la segunda vulnerabilidad, CVE-2025-32463, esta aprovecha la opción -R (chroot) de Sudo para ejecutar comandos arbitrarios como root, incluso si dichos comandos no están definidos en el archivo sudoers. Esta falla ha sido clasificada como crítica.

> *"La configuración predeterminada de Sudo es vulnerable. Aunque la falla involucra la característica chroot de Sudo, no requiere que existan reglas de Sudo definidas para el usuario. Por lo tanto, cualquier usuario local sin privilegios podría escalar sus permisos a root si el sistema tiene instalada una versión vulnerable»,* indicó Mirch.

En otras palabras, esta vulnerabilidad permite que un atacante engañe a Sudo para que cargue una biblioteca compartida manipulada, creando un archivo «/etc/nsswitch.conf» dentro de un directorio raíz personalizado, lo que puede resultar en la ejecución de código malicioso con privilegios elevados.

Miller señaló que la opción chroot será eliminada completamente en futuras versiones de Sudo, ya que permitir a los usuarios definir su propio directorio raíz es "propenso a errores".

Tras una divulgación responsable realizada el 1 de abril de 2025, ambas fallas fueron corregidas en la versión Sudo 1.9.17p1, publicada a finales del mes pasado. Diversas distribuciones de Linux han emitido sus propios avisos de seguridad, ya que Sudo viene instalado por defecto en muchas de ellas:

- CVE-2025-32462 afecta a: *AlmaLinux 8 y 9, Alpine Linux, Amazon Linux, Debian, Gentoo, Oracle Linux, Red Hat, SUSE y Ubuntu*.
- CVE-2025-32463 afecta a: *Alpine Linux, Amazon Linux, Debian, Gentoo, Red Hat, SUSE y Ubuntu*.

Se recomienda a todos los usuarios aplicar las actualizaciones correspondientes y asegurarse de que sus distribuciones de Linux estén protegidas con los paquetes más recientes.