Se descubrió una vulnerabilidad en Sudo, una de las utilidades más importantes, potentes y de uso común que viene como un comando central instalado en casi todos los sistemas operativos basados en UNIX y Linux.

La vulnerabilidad en cuestión es un problema de omisión de la política de seguridad de sudo que podría permitir que un usuario malintencionado o un programa ejecute comandos arbitrarios como root en un sistema Linux objetivo, incluso cuando la *«configuración de sudoers»* no permite explícitamente el acceso de root.

Sudo, que significa *«superusuario do»,* es un comando del sistema que permite a un usuario ejecutar aplicaciones o comandos con los privilegios de un usuario diferente sin cambiar de entorno, la mayoría de las veces, para ejecutar comandos como usuario root.

De forma predeterminada en la mayoría de las distribuciones de Linux, la palabra clave ALL en la especificación RunAs en el archivo /etc/sudoers, como se muestra en la captura de pantalla, permite a todos los usuarios en los grupos admin o sudo ejecutar cualquier comando como cualquier usuario válido en el sistema.

Sin embargo, debido a que la separación de privilegios es uno de los paradigmas de seguridad fundamentales en Linux, los administradores pueden configurar un archivo sudoers para definir qué usuarios pueden ejecutar qué comandos y qué usuarios.

Por lo tanto, incluso si un usuario ha sido restringido par ejecutar un comando específico, o cualquiera, como root, la vulnerabilidad podría permitir al usuario eludir esta política de seguridad y tomar el control completo sobre el sistema.

> *«Esto puede ser utilizado por un usuario con suficientes privilegios de sudo para ejecutar comandos como root, incluso si la especificación Runas no permite explícitamente el acceso root siempre y cuando la palabra clave ALL aparezca primero en la especificación Runas»,* dicen los desarrolladores de Sudo.

La vulnerabilidad, rastreada como CVE-2019-14287 y descubierta por Joe Vennix, de Apple Information Security, es más preocupante porque la utilidad sudo ha sido diseñada para permitir a los usuarios utilizar su propia contraseña de inicio de sesión para ejecutar comandos como un usuario diferente sin requerir su contraseña.

Esta falla puede ser explotada por un atacante para ejecutar comandos como root con el simple hecho de especificar el ID de usuario *-1* o *4294967295*.

Esto se debe a que la función que convierte la identificación de usuario en su nombre de usuario trata incorrectamente -1 o su equivalente no firmado 4294967295, como 0, que siempre es la identificación de usuario raíz.

> *«Además, debido a que el ID de usuario especificado por medio de la opción -u no existe en la base de datos de contraseñas, no se ejecutarán módulos de sesión PAM»,* agregó el investigador.

La vulnerabilidad afecta a todas las versiones de Sudo anteriores a la última versión lanzada 1.8.28, que se lanzó hoy, hace unas horas y pronto se implementará como una actualización por varias distribuciones de Linux para sus usuarios.