Joe Vennix, encargado de seguridad de Apple, encontró otra vulnerabilidad importante en la utilidad sudo que al utilizarse bajo una configuración específica, podría permitir que usuarios con pocos privilegios o programas maliciosos ejecuten comandos arbitrarios con privilegios administrativos (root) en sistemas Linux o MacOS.

Sudo es una de las utilidades más importantes, potentes y de uso común que viene como un comando central preinstalado en macOS y casi todos los sistemas operativos basados en UNIX o Linux.

El comando fue diseñado para permitir a los usuarios la ejecución de aplicaciones o comandos con los privilegios de un usuario diferente sin cambiar de entorno.

La vulnerabilidad de escalada de privilegios recientemente descubierta, rastreada como CVE-2019-18634, proviene de un problema de desbordamiento de búfer basado en pila que reside en las versiones de Sudo anteriores a 1.8.26.

Según Vennix, la falla solo puede explotarse cuando la opción *«pwfeedback»* está habilitada en el archivo de configuración de sudoers, una función que proporciona retroalimentación visual, un asterisco, cuando un usuario ingresa la contraseña en la terminal.

Cabe mencionar que la función pwfeedback no está habilitada predeterminadamente en la versión anterior de sudo o en muchos otros paquetes. Sin embargo, algunas distribuciones de Linux, como Linux Mint y Elementary OS, lo habilitan en sus archivos sudoers predeterminados.

Además, cuando pwfeedback está habilitado, la vulnerabilidad puede ser explotada por cualquier usuario, incluso sin los permisos de sudo.

> *«El error puede reproducirse pasando una entrada grande a sudo por medio de una tubería cuando solicita una contraseña. Debido a que el atacante tiene un control*

> *completo de los datos utilizados para desbordar el búfer, existe una alta probabilidad de explotabilidad»,* dijo el desarrollador de Sudo, Todd C. Miller.

Para determinar si la configuración de sudoers está siendo afectada, los usuarios pueden ejecutar el comando sudo -l en su terminal Linux o macOS para saber si la opción «pwfeedback» está habilitada y listada en la salida *«Entradas de valores predeterminados coincidentes».*

De estar habilitado, puede deshabilitarse el componente vulnerable cambiando *«Defaults pwfeedback»* a *«Defaults! Pwfeedback»* en el archivo de configuración de sudoers para evitar la explotación de la vulnerabilidad de escalada de privilegios.

Vennix informó de forma responsable la vulnerabilidad a los mantenedores de Sudo, quienes a finales de la semana pasada lanzaron la versión 1.8.31 de sudo con un parche.

> *«Si bien el error lógico también está presente en las versiones de sudo 1.8.26 a 1.8.30, no es expotable debido a un cambio en el manejo de EOF en sudo 1.8.26»*, dijo Miller.

Apple por su parte, lanzó una actualización de parche para macOS High Sierra 10.13.6, macOS Mojave 10.14.6 y macOS Catalina 10.15.2 la semana pasada.

Joe Vennix informó el año pasado una vulnerabilidad de impacto similar en Sudo que podría haber sido explotada por un atacante para ejecutar comandos como root simplemente especificando el ID de usuario «-1» o «4294967295».