



Apple implementó una solución para una vulnerabilidad en sudo crítica, en macOS Big Sur, Catalina y Mojave, que podría permitir que los usuarios locales no autenticados obtengan privilegios de root en el sistema.

«Un atacante local puede elevar sus privilegios. Este problema se solucionó actualizando a sudo versión 1.9.5p2», [dijo Apple](#).

Sudo es una utilidad común integrada en la mayoría de los sistemas operativos Unix y Linux que permite a un usuario sin privilegios de seguridad acceder y ejecutar un programa con las credenciales de otro usuario.

Rastreada como CVE-2021-3156 y también conocida como Baron Samedit, la vulnerabilidad salió a la luz por primera vez el mes pasado luego de que la compañía de auditoría de seguridad [Qualys](#), revelara la existencia de un desbordamiento de búfer basado en el montón, que según dijo, se había estado «ocultando a plena vista por casi 10 años».

La vulnerabilidad, que se introdujo en el código en julio de 2011, afecta a las versiones de sudo 1.7.7 a 1.7.10p9, 1.8.2 a 1.8.31p2 y 1.9.0 a 1.9.5p1, después de lo cual los desarrolladores lanzaron [1.8.32](#) y 1.9.5p2 para resolver el problema.

Aunque la vulnerabilidad solo puede ser explotada por un atacante que ya tenga acceso a un host vulnerable, la barrera podría evitarse fácilmente colocando malware en un dispositivo o forzando una cuenta de servicio con pocos privilegios.

En el informe de Qualys, los investigadores dijeron que lograron desarrollar múltiples variantes de exploit y obtener privilegios de root completos en Ubuntu 20.04 (Sudo 1.8.31), Debian 10 (Sudo 1.8.27) y Fedora 33 (Sudo 1.9.2).

Pero la semana pasada, el investigador de seguridad británico Matthew Hickey, descubrió que la vulnerabilidad también se extendía a la última versión de macOS Big Sur 11.2, lo que llevó a Apple a abordar la falla de seguridad.



«CVE-2021-3156 también afecta a @apple MacOS Big Sur (sin parches en la actualidad), puede habilitar la explotación del problema mediante el enlace simbólico de sudo a sudoedit y luego activar el desbordamiento del montón para escalar los privilegios a `1337 uid = 0`», dijo Hickey en Twitter el 2 de febrero.

Además de solucionar la vulnerabilidad sudo, la actualización de seguridad complementaria del martes también incluye parches para dos vulnerabilidades en Intel Graphics Driver (CVE-2021-1805 y CVE-2021-1806), que podrían hacer que una aplicación ejecute código arbitrario con privilegios del kernel.

Las vulnerabilidades, que se derivan de una escritura fuera de los límites y una condición de carrera, respectivamente, se rectificaron con una validación adicional, dijo Apple.