Investigadores de seguridad cibernética compartieron detalles sobre una vulnerabilidad de seguridad ya abordada en el sistema operativo macOS de Apple, que podría explotarse potencialmente para ejecutar aplicaciones maliciosas de una forma que puede eludir las medidas de seguridad de Apple.

La vulnerabilidad, rastreada como CVE-2022-32910, tiene sus raíces en la utilidad de archivo integrada y *«podría llevar a la ejecución de una aplicación no firmada y no certificada sin mostrar avisos de seguridad al usuario, mediante el uso de un archivo especialmente diseñado»,* dijo la firma de administración de dispositivos de Apple, Jamf.

Después de la divulgación responsable el 31 de mayo de 2022, Apple abordó el problema como parte de macOS Big Sur 11.6.8 y Monterey 12.5 lanzados el 20 de julio de 2022. El gigante tecnológico, por su parte, también revisó los avisos emitidos anteriormente a partir del 4 de octubre para agregar una entrada para la vulnerabilidad.

Apple describió el error como un problema lógico que podría permitir que un archivo de almacenamiento eluda las comprobaciones de Gatekeeper, que está diseñado para garantizar que solo se ejecute software confiable en el sistema operativo.

La tecnología de seguridad logra esto mediante la verificación que el paquete descargado es de un desarrollador legítimo y ha sido notariado por Apple, es decir, se le ha otorgado un sello de aprobación para garantizar que no haya sido manipulado de forma maliciosa.

> *«Gatekeeper también solicita la aprobación del usuario antes de abrir el software descargado por primera vez para asegurarse de que el usuario no haya sido engañado para ejecutar un código ejecutable que creía que era simplemente un archivo de datos»,* dijo Apple en su documentación de soporte.

Cabe mencionar que los archivos de almacenamiento descargados de Internet están etiquetados con el atributo extendido *«com.apple.quarantine»*, incluyendo los elementos dentro del archivo, para activar una verificación de Gatekeeper antes de la ejecución.

Pero en una peculiaridad descubierta por Jamf, Archive Utility no agrega el atributo de cuarentena a una carpeta *«al extraer un archivo que contiene dos o más archivos o carpetas en su directorio raíz».*

Por lo tanto, al crear un archivo de almacenamiento con la extensión *«exploit.app.zip»*, conduce a un escenario en el que un desarchivado da como resultado la creación de una carpeta llamada *«exploit.app»,* mientras que también carece del atributo de cuarentena.

Esta aplicación *«pasará por alto todas las comprobaciones de Gatekeeper, lo que permitirá la ejecución de un binario no certificado y/o firmado»,* dijo el investigador de Jamg, Ferdous Saljooki, quien descubrió la falla.

Los hallazgos llegan más de seis meses después de que Apple abordara otra vulnerabilidad similar en macOS Catalina, Big Sur 11.6.5 y Monterey 12.3 (CVE-2022-22616) que podría permitir que un archivo ZIP malicioso eluda las comprobaciones de Gatekeeper.