Apple solucionó recientemente una vulnerabilidad de seguridad en el sistema operativo macOS, que podría ser potencialmente aprovechada por un actor de amenazas para eludir *«trivial y confiablemente una miríada de mecanismos de seguridad fundamentales de macOS»* y ejecutar código arbitrario.

El investigador de seguridad Patrick Wardle, detalló el descubrimiento en una serie de tweets el jueves. Rastreada como CVE-2021-30853, con puntuación CVSS de 5.5, la vulnerabilidad se relaciona con un escenario en el que una aplicación macOS fraudulenta puede eludir las comprobaciones de Gatekeeper, que garantizan que solo se puedan ejecutar aplicaciones de confianza y que hayan pasado un proceso automatizado llamado *«app notarization»*.

Apple atribuye a Gordon Long, de Box, por el informe de la falla, y dijo que abordó la vulnerabilidad con controles mejorados como parte de las actualizaciones de macOS 11.6 lanzadas oficialmente el 20 de septiembre de 2021.

> *«Estos errores suelen tener un impacto especial en los usuarios de macOS de todos los días, ya que proporcionan un medio para que los autores de programas publicitarios y malware eludan los mecanismos de seguridad de macOS»*, dijo Wardle.

De forma específica, el error no solo evita a Gatekeeper, sino también a la Cuarentena de archivos y los requisitos de certificación de macOS, lo que permite que un archivo PDF aparentemente inocuo comprometa todo el sistema con solo abrirlo.

Según Wardle, el problema tiene su origen en el hecho de que una aplicación basada en un script sin firmar y no notarizada, no puede especificar explícitamente un intérprete, lo que resulta en una omisión completa.

Cabe mencionar que una directiva de intérprete shebang, por ejemplo, #!/Bin/sh o #!/Bin/bash, se usa típicamente para analizar e interpretar un programa de shell. Pero en este ataque de caso extremo, un adversario puede crear una aplicación de modo que la línea shebang se incorpore sin proporcionar un intérprete (es decir, #!) y aún así lograr que el sistema operativo subyacente inicie el script sin generar alerta alguna.

Esto ocurre porque *«macOS intentará ejecutar la aplicación basada en script sin intérprete fallida a través del shell ('/Bin/sh') después de la falta inicial de éxito»,* explicó Wardle.

En otras palabras, los actores de amenazas pueden explotar la vulnerabilidad engañando a sus objetivos para que abran una aplicación maliciosa que se puede camuflar como actualizaciones de Adobe Flash Player o versiones troyanizadas de aplicaciones legítimas como Microsoft Office, que a su vez, se pueden entregar a través de un método llamado envenenamiento de búsqueda, en el que los atacantes aumentan artificialmente la clasificación de los motores de búsqueda de los sitios web que alojan su malware para atraer a posibles víctimas.

Esta no es la primera vez que se descubren fallas en el proceso de Gatekeeper. A inicios de abril, Apple corrigió rápidamente una vulnerabilidad de día cero que luego se explotó activamente (CVE-2021-30657), que podría eludir todas las protecciones de seguridad, lo que permitiría ejecutar software no aprobado en Mac.

Después, en octubre, Microsoft reveló una vulnerabilidad denominada «Shrootless» (CVE-2021-30892), que podría aprovecharse para realizar operaciones arbitrarias, elevar privilegios a root e instalar rootkits en dispositivos comprometidos. Apple dijo que solucionó el problema con restricciones adicionales como parte de las actualizaciones de seguridad publicadas el 26 de octubre de 2021.