Microsoft reveló los detalles de una vulnerabilidad de seguridad ya parcheada en Apple macOS que podría explotarse por hackers para eludir las protecciones de seguridad impuestas para evitar la ejecución de aplicaciones maliciosas.

La vulnerabilidad, denominada Achilles (CVE-2022-42821, puntaje CVSS: 5.5), fue abordada por la compañía en macOS Ventura 13, Monterey 12.6.2 y Big Sur 11.7.2, describiéndola como un problema lógico que podría ser armado por una aplicación para eludir los controles de Gatekeeper.

> *«Las omisiones de Gatekeeper como esta podrían aprovecharse como un vector para el acceso inicial de malware y otras amenazas, y podrían ayudar a aumentar la tasa de éxito de campañas y ataques maliciosos en macOS»*, dijo Jonathan Bar Or del Microsoft 365 Defender Research Team.

Gatekeeper es un mecanismo de seguridad diseñado para garantizar que solo se ejecuten aplicaciones confiables en el sistema operativo. Esto se aplica mediante un atributo extendido llamado «*com.apple.quatantine*» que se asigna a los archivos descargados de Internet. Es análoga a la bandera Mark of the Web (MotW) en Windows.

Por lo tanto, cuando un usuario desprevenido descarga una aplicación potencialmente dañina que se hace pasar por una pieza de software legítimo, la función Gatekeeper evita que la aplicación se ejecute, ya que no está debidamente firmada y notariada por Apple.

Aún en los casos en que Apple aprueba una aplicación, a los usuarios se les muestra un aviso cuando se inicia por primera vez para solicitar su consentimiento explícito.

Dado el papel crucial que desempeña Gatekeeper en macOS, es difícil no imaginar las consecuencias de eludir la barrera de seguridad, lo que podría permitir que los atacantes implementen malware en las máquinas.

La vulnerabilidad de Achilles identificada por Microsoft explota un modelo de permisos

llamado Listas de Control de Acceso (ACL) para agregar permisos extremadamente restrictivos a un archivo descargado (es decir, «*everyone deny write, writeattr, writeextattr, write security, chown*«), lo que impide que Safari configure el atributo extendido de cuarentena.

En un escenario de ataque hipotético, un atacante podría adoptar la técnica para crear una aplicación maliciosa y alojarla en un servidor, que después podría entregarse a un posible objetivo a través de ingeniería social, anuncios maliciosos o un abrevadero.

El método también elude el modo de bloqueo recientemente introducido por Apple en macOS Ventura, una configuración restrictiva opcional para contrarrestar las vulnerabilidades de clic cero, lo que requiere que los usuarios apliquen las últimas actualizaciones para mitigar las amenazas.

> *«Las aplicaciones falsas siguen siendo uno de los principales vectores de entrada en macOS, lo que indica que las técnicas de omisión de Gatekeeper son una capacidad atractiva e incluso necesaria para que los atacantes aprovechen los ataques»,* dijo Bar Or.