Apple revisó los avisos de seguridad que publicó el mes pasado para incluir tres nuevas vulnerabilidades que afectan a iOS, iPadOS y macOS.

La primera vulnerabilidad es una condición de carrera en el componente Crash Reporter (CVE-2023-23520), que podría permitir que un hacker lea archivos arbitrarios como root. Apple dijo que abordó el problema con una validación adicional.

Las otras dos vulnerabilidades, atribuidas al investigador de Trellix, Austin Emmitt, residen en el marco de la Fundación (CVE-2023-23530 y CVE-2023-23531) y podrían convertirse en armas para lograr la ejecución del código.

«Una aplicación puede ejecutar código arbitrario fuera de su entorno limitado o con ciertos privilegios elevados», dijo Apple, y agregó que solucionó los problemas con un *«manejo de memoria mejorado».*

Las vulnerabilidades de gravedad media a alta se han parcheado en iOS 16.3, iPadOS 16.3 y macOS Ventura 13.2 que se enviaron el 23 de enero de 2023.

Trellix, en su propio informe del martes, clasificó las dos vulnerabilidades como una *«nueva clase de errores que permiten eludir la firma de código para ejecutar código arbitrario en el contexto de varias aplicaciones de plataforma, lo que lleva a una escalada de privilegios y un espace de sandbox tanto en macOS como en iOS».*

Los errores también eluden las mitigaciones que Apple implementó para abordar las vulnerabilidades de clic cero como FORCEDENTRY que fue aprovechada por el proveedor de sofware espía israelí, NSO Group para implementar Pegasus en los dispositivos de los objetivos.

Como resultado, un atacante podría explotar estas vulnerabilidades para salir de la zona de

pruebas y ejecutar código malicioso con permisos elevados, lo que podría otorgar acceso al calendario, la libreta de direcciones, los mensajes, los datos de ubicación, el historial de llamadas, la cámara, el micrófono y las fotos.

Aún más preocupante, se podría abusar de los defectos de seguridad para instalar aplicaciones arbitrarias o incluso borrar el dispositivo. Dicho esto, la explotación de las vulnerabilidades requiere que un atacante ya haya obtenido un punto de apoyo inicial.

> *«Las vulnerabilidades anteriores representan una violación significativa del modelo de seguridad de macOS e iOS, que se basa en que las aplicaciones individuales tengan un acceso detallado al subconjunto de recursos que necesitan y consulten los servicios privilegiados más altos para obtener cualquier otra cosa»,* dijo Emmitt.