Apple lanzó este jueves parches de emergencia para abordar dos vulnerabilidades de día cero en sus sistemas operativos móviles y de escritorio, que según la compañía, pueden estar siendo explotados en la naturaleza.

Las vulnerabilidades se solucionaron en las actualizaciones de iOS y iPadOS 15.4.1, macOS Monterey 12.3.1, tvOS 15.4.1 y watchOS 8.5.1. Ambas vulnerabilidades se informaron a Apple de forma anónima.

La vulnerabilidad rastreada como CVE-2022-22675, se describió como una vulnerabilidad de escritura fuera de los límites en un componente de decodificación de audio y video llamado AppleAVD, que podría permitir que una aplicación ejecute código arbitrario con privilegios de kernel.

Apple dijo que el defecto fue resuelto mejorando la verificación de límites, y agregó que es consciente de que *«este problema pudo haber sido explotada activamente».*

La última versión de macOS Monterey, además de reparar CVE-2022-22675, también incluye la corrección de CVE-2022-22674, un problema de lectura fuera de los límites en el módulo del controlador de gráficos Intel, que podría permitir que un actor malicioso lea la memoria del kernel.

El error se resolvió *«con una validación de entrada mejorada»,* dijo Apple, afirmando que existe evidencia de explotación activa, mientras retiene detalles adicionales para evitar más abusos por parte de hackers.

Las últimas actualizaciones elevan a cuatro el número total de días cero activamente explotados y parcheados por Apple desde inicio del año, sin mencionar una vulnerabilidad divulgada públicamente en la API de IndexDB (CVE-2022-22594), que podría ser un arma maliciosa para rastrear la actividad en línea de los usuarios y las identidades en el navegador web.

- CVE-2022-22587 (IOMobileFrameBuffer): Una aplicación maliciosas puede ejecutar

código arbitrario con privilegios de kernel.
- CVE-2022-22620 (WebKit): El procesamiento de contenido web creado con fines malintencionados puede provocar la ejecución de código arbitrario.

A la luz de la explotación activa de las vulnerabilidades, se recomienda encarecidamente a los usuarios de Apple iPhone, iPad y Mac, que actualicen a las últimas versiones del software lo antes posible para mitigar las posibles amenazas.

Las actualizaciones de iOS y iPad están disponibles para iPhone 6s y posteriores, iPad Pro (todos los modelos), iPad Air 2 y posteriores, iPad de 5a generación y posteriores, iPad mini 4 y posteriores y iPod touch 7a generación.