Apple ha lanzado una actualización de firmware para los AirPods que podría permitir a un atacante acceder de manera no autorizada a los auriculares.

Identificado como CVE-2024-27867, el problema de autenticación afecta a los AirPods (2ª generación y posteriores), AirPods Pro (todos los modelos), AirPods Max, Powerbeats Pro y Beats Fit Pro.

> *«Cuando tus auriculares están buscando una solicitud de conexión a uno de tus dispositivos previamente emparejados, un atacante dentro del alcance de Bluetooth podría hacerse pasar por el dispositivo de origen previsto y obtener acceso a tus auriculares»,* explicó Apple en un aviso el martes.

En otras palabras, un adversario en proximidad física podría explotar la vulnerabilidad para escuchar conversaciones privadas. Apple indicó que el problema se ha resuelto con una mejor gestión de estados.

Jonas Dreßler ha sido acreditado por descubrir y reportar la falla. Se ha corregido como parte de la Actualización de Firmware de AirPods 6A326, Actualización de Firmware de AirPods 6F8 y Actualización de Firmware de Beats 6F8.

El desarrollo ocurre dos semanas después de que el fabricante del iPhone lanzara actualizaciones para visionOS (versión 1.2) para solucionar 21 deficiencias, incluidas siete fallas en el motor del navegador WebKit.

Uno de los problemas se refiere a una falla lógica (CVE-2024-27812) que podría resultar en una denegación de servicio (DoS) al procesar contenido web. El problema se ha solucionado con una mejor gestión de archivos, indicó Apple.

El investigador de seguridad Ryan Pickren, quien reportó la vulnerabilidad, la describió como el «primer hack de computación espacial del mundo» que podría ser utilizado para *«eludir todas las advertencias y llenar forzosamente tu habitación con un número arbitrario de*

objetos 3D animados» sin interacción del usuario.

La vulnerabilidad aprovecha la falta de aplicación del modelo de permisos de Apple al usar la función ARKit Quick Look para generar objetos 3D en la habitación de una víctima. Para empeorar las cosas, estos objetos animados continúan persistiendo incluso después de salir de Safari, ya que son manejados por una aplicación separada.

> *«Además, ni siquiera requiere que esta etiqueta de anclaje haya sido 'clicada' por el usuario. Así que hacer clic en JavaScript programático (es decir, document.querySelector('a').click()) funciona sin problema. ¡Esto significa que podemos lanzar un número arbitrario de objetos 3D animados y con sonido sin ninguna interacción del usuario!»*, dijo Pickren.