Apple ha lanzado nuevas actualizaciones de iOS y iPadOS para solucionar dos vulnerabilidades de seguridad, una de las cuales podría haber permitido que la tecnología de asistencia VoiceOver leyera en voz alta las contraseñas de un usuario.

La vulnerabilidad, identificada como CVE-2024-44204, se describe como un fallo lógico en la nueva aplicación de Contraseñas, afectando a varios modelos de iPhones y iPads. El investigador de seguridad Bistrit Daha ha sido reconocido por descubrir y reportar el problema.

«Las contraseñas guardadas por el usuario podrían ser leídas en voz alta por VoiceOver», señaló Apple en un aviso publicado esta semana, añadiendo que se corrigió mediante una validación mejorada.

Los dispositivos afectados incluyen:

- iPhone XS y posteriores
- iPad Pro de 13 pulgadas
- iPad Pro de 12,9 pulgadas (desde la 3.ª generación)
- iPad Pro de 11 pulgadas (desde la 1.ª generación)
- iPad Air (desde la 3.ª generación)
- iPad (desde la 7.ª generación), y
- iPad mini (desde la 5.ª generación)

Otra vulnerabilidad corregida por Apple (CVE-2024-44207) afecta específicamente a los recién lanzados iPhone 16. Este fallo permite que se capture audio antes de que el indicador del micrófono esté activado, y está relacionado con el componente Media Session.

> *«Los mensajes de audio en la app Mensajes pueden capturar unos segundos de sonido antes de que se encienda el indicador del micrófono»,* explicó Apple.

Este problema fue solucionado con controles mejorados, y se atribuye el descubrimiento a

Michael Jimenez y a un investigador anónimo.

Se recomienda a los usuarios actualizar a iOS 18.0.1 y iPadOS 18.0.1 para proteger sus dispositivos de posibles riesgos.