Apple ha lanzado actualizaciones de seguridad para solucionar una falla que afecta a iOS, iPadOS y macOS, la cual, según confirmó la compañía, ha sido explotada activamente en entornos reales.

La vulnerabilidad de día cero, identificada como CVE-2025-43300, corresponde a un error de escritura fuera de límites en el framework ImageIO, lo que puede provocar corrupción de memoria al procesar una imagen maliciosa.

"Apple tiene conocimiento de un informe que indica que este problema pudo haber sido explotado en un ataque extremadamente sofisticado contra individuos específicos", señaló la compañía en su aviso oficial.

El fabricante del iPhone indicó que el fallo fue descubierto de manera interna y que se resolvió mediante una mejora en la validación de límites. Las versiones que corrigen el problema son las siguientes:

- iOS 18.6.2 y iPadOS 18.6.2 – iPhone XS y posteriores, iPad Pro de 13 pulgadas, iPad Pro de 12.9 pulgadas (3.ª generación y posteriores), iPad Pro de 11 pulgadas (1.ª generación y posteriores), iPad Air (3.ª generación y posteriores), iPad (7.ª generación y posteriores) y iPad mini (5.ª generación y posteriores).
- iPadOS 17.7.10 – iPad Pro de 12.9 pulgadas (2.ª generación), iPad Pro de 10.5 pulgadas y iPad (6.ª generación).
- macOS Ventura 13.7.8 – Macs con macOS Ventura.
- macOS Sonoma 14.7.8 – Macs con macOS Sonoma.
- macOS Sequoia 15.6.1 – Macs con macOS Sequoia.

Por el momento, no se conoce quién está detrás de los ataques ni quiénes han sido los objetivos, aunque es probable que la vulnerabilidad haya sido utilizada en campañas dirigidas de alta precisión.

Con esta actualización, Apple ha corregido un total de siete vulnerabilidades de día cero explotadas en ataques reales desde principios de año: CVE-2025-24085, CVE-2025-24200,

CVE-2025-24201, CVE-2025-31200, CVE-2025-31201 y CVE-2025-43200.

El mes pasado, la compañía también publicó parches para una vulnerabilidad de Safari ubicada en un componente de código abierto (CVE-2025-6558), que Google había reportado como explotada previamente como *zero-day* en el navegador Chrome.