Apple lanzó el jueves actualizaciones de seguridad para iOS, iPadOS, macOS, tvOS, watchOS y el navegador web Safari para abordar docenas de vulnerabilidades, incluyendo tres nuevos ZeroDay, que según dijo la compañía, están siendo explotadas activamente en la naturaleza.

Las tres vulnerabilidades de seguridad son:

- CVE-2023-32409: Una vulnerabilidad de WebKit que podría ser aprovechada por un hacker para salir del entorno limitado de contenido web. Se solucionó con controles de límites mejorados.
- CVE-2023-28204: Un problema de lectura fuera de los límites en WebKit que podría abusarse para revelar información confidencial al procesar contenido web. Se solucionó mejorando la validación de entrada.
- CVE-2023-32373: Un error use-after-free en WebKit que podría conducir a la ejecución de código arbitrario al procesar contenido web creado con fines malintencionados. Se solucionó mejorando la gestión de la memoria.

Apple dio crédito a Clément Lecigne del Grupo de Análisis de Amenazas (TAG) de Google y a Donncha Ó Cearbhaill, del Laboratorio de Seguridad de Amnistía Internacional por informar CVE-2023-32409. Un investigador anónimo ha sido reconocido por informar los otros dos problemas.

Cabe mencionar que tanto CVE-2023-2804 como CVE-2023-32373 se parchearon como parte de las actualizaciones de Rapid Security Response para iOS 16.4.1 y iPadOS 16.4.1, que la compañía lanzó al iniciar el mes.

Actualmente no hay detalles técnicos adicionales sobre las vulnerabilidades, la naturaleza de los ataques o la identidad de los hackers que pueden estar explotándolos.

Debido a esto, las vulnerabilidades se han aprovechado históricamente como parte de intrusiones altamente dirigidas para desplegar spyware en los dispositivos de disidentes, periodistas y activistas de derechos humanos.

Las últimas actualizaciones están disponibles para los siguientes dispositivos y sistemas operativos:

- iOS 16.5 y iPadOS 16.5: iPhone 8 y posteriores, iPad Pro (todos los modelos), iPad Air de 3.ª generación y posteriores, iPad de 5.ª generación y posteriores y iPad mini de 5.ª generación y posteriores
- iOS 15.7.6 y iPadOS 15.7.6: iPhone 6s (todos los modelos), iPhone 7 (todos los modelos), iPhone SE (1.ª generación), iPad Air 2, iPad mini (4.ª generación) y iPod touch (7.ª generación)
- macOS Ventura 13.4: – macOS Ventura
- tvOS 16.5: – Apple TV 4K (todos los modelos) y Apple TV HD
- watchOS 9.5: – Apple Watch Serie 4 y posterior
- Safari 16.5: macOS Big Sur y macOS Monterey

Hasta ahora, Apple reparó un total de seis vulnerabilidades de día cero explotadas activamente desde el comienzo de 2023. A inicios de febrero, la compañía solucionó una vulnerabilidad de WebKit (CVE-2023-23529) que podría conducir a la ejecución remota de código.

Después, en abril, envió correcciones para dos vulnerabilidades (CVE-2023-28205 y CVE-2023-28206), que permitían la ejecución de código con privilegios elevados. A Lecigne y Ó Cearbhaill se les atribuyó el informe de las vulnerabilidades.