Apple emitió el jueves actualizaciones de seguridad de emergencia para iOS, iPadOS, macOS y watchOS para abordar dos vulnerabilidades zero-day que se han aprovechado en la vida real para distribuir el software espía Pegasus de la empresa mercenaria NSO Group.

Las cuestiones se vulnerabilidades de la siguiente manera:

- CVE-2023-41061: Un problema de validación en Wallet que podría resultar en la ejecución de código no autorizado al manipular un adjunto maliciosamente elaborado.
- CVE-2023-41064: Un problema de desbordamiento de búfer en el componente Image I/O que podría resultar en la ejecución de código no autorizado al procesar una imagen maliciosamente elaborada.

Mientras que CVE-2023-41064 fue descubierto por el equipo de Citizen Lab en la Universidad de Toronto, Escuela Munk, CVE-2023-41061 fue identificado internamente por Apple, con apoyo de Citizen Lab.

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

- iOS 16.6.1 e iPadOS 16.6.1: iPhone 8 y modelos posteriores, iPad Pro (todos los modelos), iPad Air de tercera generación en adelante, iPad de quinta generación en adelante y iPad mini de quinta generación en adelante.
- macOS Ventura 13.5.2: dispositivos macOS que ejecutan macOS Ventura.
- watchOS 9.6.2: Apple Watch Series 4 y modelos posteriores.

En un aviso separado, Citizen Lab reveló que las dos vulnerabilidades zero-day se han utilizado como parte de una cadena de explotación de iMessage sin intervención llamada BLASTPASS para instalar Pegasus en iPhones completamente actualizados que ejecutan iOS 16.6.

> *«La cadena de explotación fue capaz de comprometer iPhones que ejecutan la versión más reciente de iOS (16.6) sin ningún tipo de interacción por parte de la*

> *víctima. La explotación implicaba adjuntos de PassKit que contenían imágenes maliciosas enviadas desde una cuenta de iMessage del atacante a la víctima»,* declaró el laboratorio interdisciplinario.

Detalles técnicos adicionales sobre las deficiencias se mantienen en secreto debido a la explotación activa. Sin embargo, se informa que la explotación elude el marco de seguridad BlastDoor establecido por Apple para mitigar los ataques sin intervención.

«Este último hallazgo demuestra una vez más que la sociedad civil es objeto de exploits altamente sofisticados y software espía mercenario», señaló Citizen Lab, agregando que se descubrieron las deficiencias la semana pasada al examinar el dispositivo de un individuo no identificado empleado por una organización de la sociedad civil con oficinas internacionales en Washington D.C.

Hasta el momento, Cupertino ha solucionado un total de 13 vulnerabilidades zero-day en su software desde el comienzo del año. Las últimas actualizaciones también llegan más de un mes después de que la empresa enviara correcciones para una vulnerabilidad de kernel que estaba siendo explotada activamente (CVE-2023-38606).

La noticia sobre los zero-days surge en un momento en que se cree que el gobierno chino ha ordenado una prohibición que prohíbe a los funcionarios del gobierno central y estatal el uso de iPhones y otros dispositivos de marcas extranjeras para trabajar, en un intento de reducir la dependencia de la tecnología extranjera, en medio de una creciente guerra comercial entre China y Estados Unidos.

> *«La razón real [de la prohibición] es la ciberseguridad (no es una sorpresa). Los iPhones tienen la reputación de ser los teléfonos más seguros... pero en realidad, los iPhones no son seguros en absoluto contra la vigilancia simple»*, señaló Zuk Avraham, investigador de seguridad y fundador de Zimperium, en una publicación en X (anteriormente Twitter).

> *«¿No me crees? Solo observa la cantidad de ataques sin intervención que empresas comerciales como NSO han realizado a lo largo de los años para comprender que prácticamente no hay nada que un individuo, una organización o un gobierno puedan hacer para protegerse contra la ciberespionaje a través de iPhones».*