Apple lanzó el miércoles actualizaciones de seguridad para abordar una reciente vulnerabilidad de día cero en los sistemas operativos iOS y iPadOS, que según informó, ha estado siendo activamente explotada en el entorno real.

Identificada como CVE-2023-42824, esta vulnerabilidad en el núcleo del sistema podría ser utilizada por un atacante local para elevar sus propios privilegios. La compañía fabricante del iPhone indicó que ha solucionado este problema mediante mejoras en las verificaciones.

> *«Apple ha tomado conocimiento de un informe que sugiere que este problema pudo haber sido aprovechado en versiones anteriores a iOS 16.6»,* señaló la empresa en un breve comunicado.

Aunque actualmente no se disponen de detalles adicionales sobre la naturaleza de los ataques ni sobre la identidad de los actores de amenazas que los llevaron a cabo, parece probable que la explotación con éxito dependa de que el atacante ya haya logrado una posición inicial de alguna otra manera.

La última actualización de Apple también soluciona CVE-2023-5217, que afecta al componente WebRTC y que Google describió la semana pasada como un desbordamiento de búfer basado en la memoria en el formato de compresión VP8 en libvpx.

Estos parches, denominados iOS 17.0.3 e iPadOS 17.0.3, están disponibles para los siguientes dispositivos:

- iPhone XS y modelos posteriores.
- iPad Pro de 12.9 pulgadas desde la 2ª generación en adelante, iPad Pro de 10.5 pulgadas, iPad Pro de 11 pulgadas de la 1ª generación en adelante, iPad Air desde la 3ª generación en adelante, iPad desde la 6ª generación en adelante y iPad mini desde la 5ª generación en adelante.

Con este último desarrollo, Apple ha abordado un total de 17 vulnerabilidades de día cero

que estaban siendo activamente explotadas en su software desde principios de año.

Esto ocurre dos semanas después de que Cupertino lanzara correcciones para resolver tres problemas (CVE-2023-41991, CVE-2023-41992 y CVE-2023-41993), los cuales, según se informa, habrían sido utilizados por un proveedor de spyware israelí llamado Cytrox para introducir el malware Predator en el iPhone perteneciente al exmiembro del parlamento egipcio Ahmed Eltantawy a principios de este año.

Un punto importante a mencionar aquí es que CVE-2023-41992 también se refiere a una debilidad en el núcleo del sistema que permite a atacantes locales obtener una escalada de privilegios.

No está claro de inmediato si estas dos vulnerabilidades están relacionadas entre sí o si CVE-2023-42824 es una solución que evita la corrección de CVE-2023-41992.

Recientemente, Sekoia señaló en un análisis que encontró similitudes en la infraestructura utilizada por los clientes de Cytrox (también conocido como Lycantrox) y de otra empresa comercial de spyware llamada Candiru (también conocida como Karkadann), probablemente debido a que ambas hacen uso de tecnologías de spyware.

> *«La infraestructura utilizada por Lycantrox consta de servidores privados virtuales (VPS) alojados en diversos sistemas autónomos»,* explicó la firma francesa de ciberseguridad, con cada cliente pareciendo operar sus propias instancias de VPS y gestionar sus propios nombres de dominio asociados.

Se recomienda a los usuarios que puedan estar en riesgo de ser blanco de ataques que activen el Modo de Bloqueo para reducir la exposición a las posibles explotaciones de spyware realizado por actores no gubernamentales.