Google ha alertado sobre una vulnerabilidad de seguridad que afecta a su sistema operativo Android y que ha sido activamente explotada en entornos reales.

La vulnerabilidad, registrada como CVE-2024-43093, se describe como un problema de escalada de privilegios en el componente de la infraestructura de Android. Este fallo podría permitir el acceso no autorizado a los directorios «Android/data», «Android/obb» y «Android/sandbox», así como a sus subdirectorios, según lo documenta un mensaje de compromiso de código.

Aún no se han revelado detalles específicos sobre cómo se está utilizando esta vulnerabilidad en ataques concretos, pero Google señaló en su boletín mensual que existen indicios de que *«podría estar siendo explotada de manera limitada y dirigida».*

La empresa también ha destacado la vulnerabilidad CVE-2024-43047, un error de seguridad que ya fue parcheado en los chipsets de Qualcomm y que también ha sido explotado activamente. Este problema de «uso después de liberación» (use-after-free) en el Servicio del Procesador de Señales Digitales (DSP) podría llevar a la corrupción de memoria si es explotado exitosamente.

El mes pasado, el fabricante de chips Qualcomm agradeció al investigador de Google Project Zero, Seth Jenkins, y a Conghui Wang por identificar el problema, así como al Laboratorio de Seguridad de Amnistía Internacional por confirmar la actividad en el entorno real.

El comunicado no ofrece detalles sobre la actividad de explotación ni sobre cuándo comenzó, aunque es posible que haya sido empleada en ataques de spyware altamente dirigidos a miembros de la sociedad civil.

Tampoco se sabe si ambas vulnerabilidades se han combinado para formar una cadena de explotación que eleve privilegios y permita la ejecución de código.

La vulnerabilidad CVE-2024-43093 es la segunda falla activa en el Marco de Android después de la CVE-2024-32896, que Google solucionó en junio y septiembre de 2024. Aunque

inicialmente solo fue reparada en dispositivos Pixel, posteriormente la empresa confirmó que esta falla afecta a un espectro más amplio de dispositivos Android.