Google publicó el lunes sus actualizaciones de seguridad mensuales para el sistema operativo Android, incluyendo dos vulnerabilidades que, según indicó, han sido explotadas activamente.

El parche corrige un total de 107 fallos de seguridad distribuidos en diversos componentes, entre ellos Framework, System, Kernel, así como módulos de Arm, Imagination Technologies, MediaTek, Qualcomm y Unison.

Las dos fallas de alta gravedad que han sido explotadas se enumeran a continuación:

"CVE-2025-48633 – Una vulnerabilidad de divulgación de información en Framework"
"CVE-2025-48572 – Una vulnerabilidad de elevación de privilegios en Framework"

Como es habitual, Google no ha proporcionado detalles adicionales sobre la naturaleza de los ataques que las aprovechan, si se han combinado entre sí o si se han utilizado por separado, ni el alcance de estas actividades. Tampoco se sabe quién está detrás de los ataques.

No obstante, la empresa tecnológica reconoció en su aviso que existen indicios de que *"podrían estar siendo explotadas de forma limitada y dirigida"*.

Google también solucionó, como parte de las actualizaciones de diciembre de 2025, una vulnerabilidad crítica en el componente Framework (*CVE-2025-48631*), la cual podría provocar una denegación de servicio (DoS) remota sin requerir permisos de ejecución adicionales.

El boletín de seguridad de diciembre incluye dos niveles de parche, *2025-12-01* y *2025-12-05*, lo que permite a los fabricantes de dispositivos abordar con mayor rapidez ciertas vulnerabilidades comunes en todos los equipos Android. Se recomienda a los usuarios actualizar sus dispositivos al nivel de parche más reciente tan pronto como las correcciones estén disponibles.

Este avance llega tres meses después de que la compañía publicara soluciones para mitigar

dos fallos explotados activamente en el kernel de Linux (*CVE-2025-38352*, puntuación CVSS: 7.4) y en Android Runtime (*CVE-2025-48543*, puntuación CVSS: 7.4), que podían derivar en una escalada local de privilegios.