Samsung ha publicado sus actualizaciones de seguridad mensuales para Android, incluyendo la corrección de una vulnerabilidad que, según la compañía, ha sido utilizada en ataques de día cero.

La falla, identificada como CVE-2025-21043 (con una puntuación CVSS de 8.8), está relacionada con una escritura fuera de los límites de memoria que podría permitir la ejecución arbitraria de código.

"La escritura fuera de límites en libimagecodec.quram.so, antes de la versión SMR Sep-2025 Release 1, permite a atacantes remotos ejecutar código arbitrario", señaló Samsung en un aviso. *"El parche corrigió la implementación incorrecta."*

De acuerdo con un informe de 2020 de Google Project Zero, libimagecodec.quram.so es una librería de análisis de imágenes de código cerrado desarrollada por Quramsoft, que añade compatibilidad con diversos formatos gráficos.

El problema, catalogado como crítico por la compañía surcoreana, impacta a Android en sus versiones 13, 14, 15 y 16. La vulnerabilidad fue reportada de manera privada a Samsung el 13 de agosto de 2025.

La empresa no ofreció detalles sobre el modo en que la falla ha sido aprovechada en los ataques ni sobre los actores detrás de ellos. No obstante, reconoció que *"existe un exploit de esta vulnerabilidad en entornos reales."*

Este hecho ocurre poco después de que Google informara que resolvió dos fallos de seguridad en Android (CVE-2025-38352 y CVE-2025-48543), los cuales, según indicó, también habían sido explotados en ataques dirigidos.