Google ha publicado actualizaciones de seguridad para corregir múltiples fallos en Android, entre ellos dos vulnerabilidades de Qualcomm que han sido *marcadas como explotadas activamente en entornos reales*.

Las fallas incluyen *CVE-2025-21479* (puntuación CVSS: 8.6) y *CVE-2025-27038* (puntuación CVSS: 7.5), ambas divulgadas junto con *CVE-2025-21480* (puntuación CVSS: 8.6) por el fabricante de chips en junio de 2025.

CVE-2025-21479 corresponde a una vulnerabilidad de autorización incorrecta en el componente de Gráficos que podría provocar corrupción de memoria debido a la ejecución no autorizada de comandos en el microcódigo de la GPU.

Por su parte, *CVE-2025-27038* es una vulnerabilidad de tipo *use-after-free* en el mismo componente gráfico, que puede derivar en corrupción de memoria al renderizar gráficos mediante los controladores de GPU Adreno en Chrome.

Aún no se han revelado detalles sobre cómo se han utilizado estas vulnerabilidades en ataques reales, aunque Qualcomm indicó en su momento que *"hay indicios por parte del Grupo de Análisis de Amenazas de Google de que CVE-2025-21479, CVE-2025-21480 y CVE-2025-27038 podrían estar siendo explotadas de forma limitada y dirigida"*.

Dado que fallos similares en chips de Qualcomm han sido aprovechados anteriormente por proveedores de *spyware* comercial como Variston y Cy4Gate, se sospecha que estas vulnerabilidades también podrían haber sido explotadas en un contexto similar.

Las tres vulnerabilidades ya han sido incorporadas al catálogo de *Vulnerabilidades Conocidas y Explotadas (KEV)* de la Agencia de Ciberseguridad y Seguridad de Infraestructura de EE. UU. (CISA), lo cual obliga a las agencias federales a aplicar los parches antes del 24 de junio de 2025.

El parche de agosto de 2025 de Google también corrige dos fallos de escalada de privilegios de alta gravedad en el Android Framework (*CVE-2025-22441* y *CVE-2025-48533*), así como

una vulnerabilidad crítica en el componente del Sistema (*CVE-2025-48530*) que podría permitir la ejecución remota de código al combinarse con otros fallos, sin requerir permisos adicionales ni interacción del usuario.

El gigante tecnológico ha liberado dos niveles de parches, *2025-08-01* y *2025-08-05*, siendo este último el que también incluye correcciones para componentes de código cerrado y de terceros, como los de Arm y Qualcomm. Se recomienda a los usuarios de dispositivos Android instalar estas actualizaciones tan pronto como estén disponibles para protegerse contra posibles amenazas.