Qualcomm ha publicado actualizaciones de seguridad para corregir casi veinte vulnerabilidades que afectan tanto a componentes propietarios como de código abierto, incluyendo una que ya está siendo explotada activamente.

La vulnerabilidad de alta gravedad, identificada como CVE-2024-43047 (puntuación CVSS: 7.8), ha sido descrita como un error de uso después de liberación («user-after-free») en el Servicio del Procesador de Señal Digital (DSP). Este fallo podría provocar *«corrupción de memoria al gestionar los mapas de memoria de HLOS.»*

Qualcomm ha reconocido a los investigadores Seth Jenkins, de Google Project Zero, y Conghui Wang por descubrir esta vulnerabilidad, así como al Laboratorio de Seguridad de Amnistía Internacional por confirmar su explotación en entornos reales.

> *«El Grupo de Análisis de Amenazas de Google ha señalado que CVE-2024-43047 podría estar siendo explotada de manera limitada y dirigida»*, señaló el fabricante en un comunicado.
>
> *«Los parches para solucionar este problema en el controlador FASTRPC ya se han distribuido a los fabricantes (OEM), acompañados de una recomendación firme de implementar la actualización en los dispositivos afectados lo antes posible.»*

Aunque aún no se conoce el alcance total de los ataques ni su impacto, es posible que esta vulnerabilidad haya sido utilizada en ataques de spyware contra miembros de la sociedad civil.

El parche de octubre también soluciona una vulnerabilidad crítica en el Administrador de Recursos WLAN (CVE-2024-33066, puntuación CVSS: 9.8), ocasionada por una validación de entradas incorrecta que podría provocar corrupción de memoria.

Este lanzamiento coincide con la publicación del boletín de seguridad mensual de Google

para Android, el cual corrige 28 vulnerabilidades adicionales, incluyendo problemas en componentes de Imagination Technologies, MediaTek y Qualcomm.