El fabricante de chips Qualcomm ha emitido actualizaciones de seguridad para abordar 17 vulnerabilidades en diversos componentes, al mismo tiempo que advierte sobre la explotación activa de tres vulnerabilidades zero-day adicionales.

De las 17 debilidades, tres son consideradas críticas, 13 tienen una calificación de alta importancia y una se considera de gravedad media.

> La compañía de semiconductores menciona en un aviso que *«existen indicios del Grupo de Análisis de Amenazas de Google y Google Project Zero de que CVE-2023-33106, CVE-2023-33107, CVE-2022-22071 y CVE-2023-33063 podrían estar siendo objeto de una explotación limitada y dirigida».*

> *«Parches para los problemas que afectan a los controladores de Adreno GPU y Compute DSP están disponibles, y se ha notificado a los fabricantes originales con una sólida recomendación de implementar las actualizaciones de seguridad lo más pronto posible».*

CVE-2022-22071 (puntuación CVSS: 8.4), descrito como un problema de uso posterior a la liberación en la Plataforma de OS Automotriz, fue originalmente corregido por la empresa como parte de sus actualizaciones en mayo de 2022.

Aunque se esperan detalles adicionales sobre las otras deficiencias para diciembre de 2023, esta revelación coincide con el día en que Arm lanzó parches para una falla de seguridad en el controlador de Kernel Mali GPU (CVE-2023-4211) que también ha sido objeto de una explotación limitada y dirigida.

Las actualizaciones de octubre de 2023 de Qualcomm también abordan tres problemas críticos, aunque no hay evidencia de que se hayan utilizado en la naturaleza:

- CVE-2023-24855 (puntuación CVSS: 9.8) – Corrupción de memoria en el Módem al procesar la configuración relacionada con la seguridad antes del intercambio de seguridad AS.
- CVE-2023-28540 (puntuación CVSS: 9.1) – Problema criptográfico en el Modem de Datos debido a una autenticación incorrecta durante el handshake de TLS.
- CVE-2023-33028 (puntuación CVSS: 9.8) – Corrupción de memoria en el Firmware WLAN al realizar una copia de memoria de la caché pmk.

Se recomienda a los usuarios aplicar las actualizaciones proporcionadas por los fabricantes originales (OEM) tan pronto como estén disponibles.