Google ha alertado sobre una vulnerabilidad de seguridad en el Firmware de Pixel que ha sido aprovechada en el mundo real como un zero-day.

La vulnerabilidad de alta severidad, conocida como CVE-2024-32896, ha sido identificada como un problema de elevación de privilegios en el Firmware de Pixel.

La empresa no proporcionó detalles adicionales sobre la naturaleza de los ataques que están explotando esta vulnerabilidad, pero mencionó que *«hay indicios de que CVE-2024-32896 está siendo objeto de explotación limitada y específica».*

La actualización de seguridad de junio de 2024 aborda un total de 50 vulnerabilidades de seguridad, incluyendo cinco relacionadas con diversos componentes de los chipsets Qualcomm.

Entre los problemas destacados que se han corregido se encuentra un problema de denegación de servicio (DoS) que afecta al Módem, y múltiples fallas de divulgación de información que afectan a GsmSs, ACPM y Trusty.

Estas actualizaciones están disponibles para los dispositivos Pixel compatibles, como Pixel 5a con 5G, Pixel 6a, Pixel 6, Pixel 6 Pro, Pixel 7, Pixel 7 Pro, Pixel 7a, Pixel 8, Pixel 8 Pro, Pixel 8a y Pixel Fold.

En abril anterior, Google solucionó dos vulnerabilidades en los componentes del cargador de arranque y del firmware (CVE-2024-29745 y CVE-2024-29748) que fueron utilizadas por empresas forenses para robar información sensible.

Luego, la semana pasada, Arm alertó a los usuarios sobre una vulnerabilidad relacionada con la memoria (CVE-2024-4610) en los controladores del kernel de GPU Bifrost y Valhall que ha sido objeto de explotación activa.