Google ha lanzado actualizaciones mensuales de seguridad para Android para abordar una serie de vulnerabilidades, incluyendo un defecto de día cero que, según la empresa, podría haber sido explotado en la vida real.

Identificado como CVE-2023-35674, esta vulnerabilidad de alta gravedad se describe como un caso de aumento de privilegios que afecta al marco de trabajo de Android.

«Existen indicios de que CVE-2023-35674 podría estar siendo aprovechado de manera limitada y específica», mencionó la compañía en su Boletín de Seguridad de Android para septiembre de 2023, sin entrar en detalles adicionales.

La actualización también resuelve tres otras vulnerabilidades de aumento de privilegios en el marco de trabajo, y el gigante de las búsquedas señala que la más crítica de estas cuestiones *«podría dar lugar a un aumento de privilegios local sin necesidad de privilegios de ejecución adicionales»* sin requerir interacción del usuario.

Google informó que también ha solucionado una vulnerabilidad de seguridad crítica en el componente del Sistema que podría conducir a la ejecución de código remoto sin necesitar la intervención de la víctima.

> *«La evaluación de la gravedad se basa en el impacto que podría tener la explotación de la vulnerabilidad en un dispositivo afectado, suponiendo que las medidas de mitigación de la plataforma y el servicio se encuentren desactivadas por motivos de desarrollo o si se superan con éxito»*, añadió.

En total, Google ha corregido 14 defectos en el módulo del Sistema y dos insuficiencias en el componente MediaProvider, este último será distribuido como una actualización del sistema a través de Google Play.