Google ha lanzado sus actualizaciones de seguridad mensuales para el sistema operativo Android con el objetivo de corregir una vulnerabilidad conocida que, según informes, ha sido explotada activamente en entornos reales.

La vulnerabilidad, clasificada como de alta gravedad y registrada como CVE-2024-32896 (con una puntuación CVSS de 7.8), está relacionada con un caso de escalada de privilegios en el componente del Framework de Android.

Según la descripción del problema en la Base Nacional de Datos de Vulnerabilidades (NVD) del NIST, se trata de un error lógico que podría permitir una escalada local de privilegios sin la necesidad de permisos de ejecución adicionales.

> *«Existen indicios de que CVE-2024-32896 podría estar siendo explotado de manera limitada y específica»,* señaló Google en su Boletín de Seguridad de Android de septiembre de 2024.

Es importante destacar que CVE-2024-32896 fue revelada por primera vez en junio de 2024, afectando inicialmente solo a los dispositivos de la línea Pixel, propiedad de Google.

No se han divulgado detalles sobre cómo se está explotando esta vulnerabilidad en el entorno real, aunque los desarrolladores de GrapheneOS indicaron que CVE-2024-32896 soluciona parcialmente el problema relacionado con CVE-2024-29748, otra falla de Android que ha sido utilizada por empresas forenses.

Google confirmó que el impacto de CVE-2024-32896 va más allá de los dispositivos Pixel, afectando a todo el ecosistema de Android, y que están colaborando con los fabricantes de equipos originales (OEM) para aplicar las correcciones donde sea necesario.

> *«Para explotar esta vulnerabilidad se requiere acceso físico al dispositivo, y esto interrumpe el proceso de restablecimiento de fábrica. Serían necesarios otros*

> *exploits adicionales para comprometer el dispositivo por completo»*, indicó Google en su comunicado.
>
> *«Estamos dando prioridad a las correcciones para otros socios OEM de Android y las implementaremos tan pronto como estén disponibles. Como medida de seguridad, se recomienda a los usuarios que siempre mantengan sus dispositivos actualizados con las últimas versiones de seguridad disponibles».*