Google ha publicado sus actualizaciones de seguridad mensuales para el sistema operativo Android, resolviendo 46 nuevas vulnerabilidades de software. Entre estas, se han identificado tres vulnerabilidades que están siendo explotadas activamente en ataques específicos.

Una de las vulnerabilidades, identificada como CVE-2023-26083, es una falla de fugas de memoria que afecta al controlador de GPU Arm Mali en los chips Bifrost, Avalon y Valhall. Esta vulnerabilidad en particular fue aprovechada en un ataque previo que permitió la infiltración de spyware en dispositivos Samsung en diciembre de 2022.

Esta vulnerabilidad fue considerada lo suficientemente grave como para que la Agencia de Ciberseguridad e Infraestructura (CISA) emitiera una orden de parcheo para agencias federales en abril de 2023.

Otra vulnerabilidad significativa, conocida como CVE-2021-29256, es un problema de alta gravedad que afecta a versiones específicas de los controladores de kernel de GPU Arm Mali Bifrost y Midgard. Esta falla permite a un usuario sin privilegios obtener acceso no autorizado a datos sensibles y escalar privilegios al nivel de root.

La tercera vulnerabilidad explotada, CVE-2023-2136, es un fallo crítico descubierto en Skia, la biblioteca de gráficos 2D de código abierto de Google. Inicialmente se reveló como una vulnerabilidad de día cero en el navegador Chrome y permite a un atacante remoto que ha tomado el control del proceso de renderizado realizar una evasión del entorno de seguridad y ejecutar código remoto en dispositivos Android.

Además de esto, el boletín de seguridad de Android de julio de Google destaca otra vulnerabilidad crítica, CVE-2023-21250, que afecta al componente del sistema Android. Este problema puede provocar la ejecución remota de código sin interacción del usuario ni privilegios de ejecución adicionales, lo que lo hace particularmente peligroso.

Estas actualizaciones de seguridad se despliegan en dos niveles de parches. El nivel de parche inicial, disponible el 1 de julio, se centra en los componentes principales de Android y aborda 22 defectos de seguridad en los componentes del Marco y del Sistema.

El segundo nivel de actualización, lanzado el 5 de julio, se enfoca en los componentes del kernel y en los componentes de código cerrado, abordando 20 vulnerabilidades en los componentes Kernel, Arm, Imagination Technologies, MediaTek y Qualcomm.

Es importante tener en cuenta que el impacto de las vulnerabilidades resueltas puede extenderse más allá de las versiones de Android compatibles (11, 12 y 13), potencialmente afectando a versiones antiguas del sistema operativo que ya no reciben soporte oficial.

Google también ha lanzado parches de seguridad específicos para sus dispositivos Pixel, que tratan 14 vulnerabilidades en los componentes Kernel, Pixel y Qualcomm. Dos de estas debilidades críticas podrían resultar en ataques de elevación de privilegios y ataques de denegación de servicio.